DATE: April 1, 2021

CHAPTER 400 – INVESTIGATIONS

TABLE OF CONTENTS

DATE: October 1, 2020

CHAPTER 400 - INVESTIGATIONS

(400)-10 Authority and Organization

10.1.1 Abbreviations and Acronyms.

Abbreviation/Acronym	Meaning
AD	Assistant Director
AFIS	Automated Fingerprint Identification System
AG	Attorney General of the United States
AIG	Assistant Inspector General
AIGA	Associate Inspector General for Audit
AIGI	Assistant Inspector General for Investigations
AIMS	Audit Information Management System
AIT	Assistant Special Agent in Charge In-Service Training
ANAB	American National Standards Institute American Society for Quality National Accreditation
ASAC	Assistant Special Agent in Charge
ASTM	American Society for Testing and Materials
ATLAS	Audit Trail Lead Analysis System
AUSA	Assistant United States Attorney
BART	Billing Analysis Reporting Tool

Abbreviation/Acronym	Meaning
BBP	Bloodborne Pathogen
BDA	Blanket Declination Agreement
BEPR	Board on Employee Professional Responsibility
BOP	Bureau of Prisons
BSA	Bank Secrecy Act
CAF	Centralized Authorization File
CBP	Customs and Border Protection
CBRS	Currency Banking Retrieval System
CCID	Cybercrime Investigations Division
CCTV	Closed-Circuit Television
CD-R	Compact Disk - Recordable
C.F.R.	Code of Federal Regulation
CIC	Cyber Investigative Cadre
CICD	Criminal Intelligence and Counterterrorism Division
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CITP	Criminal Investigator Training Program
CJIS	Criminal Justice Information Services
CMIR	Currency and Monetary Instruments
CMT	Complaint Management Team

Abbreviation/Acronym	Meaning
COOP	Continuity of Operations
CPA	Certified Public Accountant
CPR	Cardio-pulmonary Resuscitation
CRIMES	Criminal Results Management System
CS	Confidential Source
CSIRC	Computer Security Incident Response Center
CTR	Currency Transaction Report
CTRC	Currency Transaction Report Casino
CVRA	Crime Victims' Rights Act
DAIGI	Deputy Assistant Inspector General for Investigations
DCITA	Defense Cyber Investigative Training Academy
DEA	Drug Enforcement Administration
DEO	Deputy Ethics Officer
DFC	Divisional Firearms, Agent Safety, and Tactics Coordinator
DFS	Digital Forensic Support
DIGA	Deputy Inspector General for Audit
DIGI	Deputy Inspector General for Investigations
DIP	Digital Image Processing
DIR	Director

Abbreviation/Acronym	Meaning
DLN	Document Locator Number
DNA	Deoxyribonucleic Acid
DNR	Dialed Number Recorder
DO	Delegation Order
DOB	Date of Birth
DOJ	Department of Justice
DOL	Department of Labor
DOT	Department of Transportation
DSAC	Deputy Special Agent in Charge
DTA	Divisional Technical Agent
DTC	Defensive Tactics Coordinator
DVD-R	Digital Versatile Disk - Recordable
DVWC	Division Victim Witness Coordinator
EAP	Employee Assistance Program
ECCO	Employee Conduct and Compliance Office
EEO	Equal Employment Opportunity
EEOC	Equal Employment Opportunity Commission
EIN	Employer Identification Number
EKG	Electrocardiogram
EOD	Entered on Duty
EPF	Employee Performance File

Abbreviation/Acronym	Meaning
EPIC	El Paso Intelligence Center
ETC	Enforcement and Technical Operations
FAA	Federal Aviation Administration
FAX	Facsimile
FAST	Firearms, Agent Safety and Tactics Program
FBAR	Report of Foreign Bank and Financial Accounts
FBI	Federal Bureau of Investigation
FCRA	Fair Credit Reporting Act
FDSL	Forensic and Digital Science Laboratory
FECA	Federal Employees Compensation Act
FI	Firearms Instructor
FICA	Federal Insurance Contributions Act
FinCEN	Financial Crimes Enforcement Network
FIP	Fictitious Identity Package
FIRTP	Firearms Instructor Refresher Training Program (FLETC)
FITP	Firearms Instructor Training Program (FLETC)
FLETC	Federal Law Enforcement Training Center

Abbreviation/Acronym	Meaning
FMFIA	Federal Managers Financial Integrity Act
FMR	Federal Management Regulations
FMS	Financial Management Service
FMSS	Facilities Management and Security Services
FOH	Federal Occupational Health
FOIA	Freedom of Information Act
FPS	Federal Protective Service
FRB	Federal Reserve Bank
FRCP	Federal Rules of Criminal Procedure
FRE	Federal Rules of Evidence
FSD	Fraud and Schemes Division
FY	Fiscal Year
GAO	Government Accountability Office
GLFD	Great Lakes Field Division
GOV	Government Owned Vehicle
GPRA	Government Performance and Results Act
GPS	Global Positioning System
GSA	General Services Administration
GSFD	Gulf States Field Division
HBV	Hepatitis B

Abbreviation/Acronym	Meaning
HIP	Health Improvement Program
HTW	Home-to-Work
IAFIS	Integrated Automated Fingerprint Identification System
I&E	Office of Inspections and Evaluations
IALEFI-Q	International Association of Law Enforcement Firearms Instructors-Qualification
ICP	Instructor Cadre Program
IDP	Individual Development Plan
IDRS	Integrated Data Retrieval System
IG	Inspector General
IG Act	Inspector General Act of 1978, as amended, 5 U.S.C. Appendix 3
IMDS	Internal Management Document System
IMIS	Investigations Management Information System
IRA	Individual Right of Action
IRC	Internal Revenue Code
IRM	Internal Revenue Manual
IRP	Information Returns Processing
IRS	Internal Revenue Service
ITMS	Integrated Talent Management System

Abbreviation/Acronym	Meaning
ITNTA	Instructor Techniques for Non-Lethal Training Ammunition
LEAP	Law Enforcement Availability Pay
LECTITP	Law Enforcement Control Tactics Instructor Training Program
LEO	Law Enforcement Officer
LERTP	Law Enforcement Rifle Training Program
LII	Local Investigative Initiative
LIMS	Laboratory Information Management System
LOM	Laboratory Operating Manual
MAFD	Mid Atlantic Field Division
Manual	TIGTA Operations Manual
MAPS	Moneys and Property System
MCC	Martinsburg Computing Center
MOU	Memorandum of Understanding
MSPB	Merit Systems Protection Board
M&P	Military and Police
NCIC	National Crime Information Center
NEFD	North East Field Division
NFC	National FAST Coordinator
NII	National Investigative Initiatives
NIJ	National Institute of Justice

Abbreviation/Acronym	Meaning
NIOC	National Investigative Operations Coordinator
NLETS	National Law Enforcement Telecommunications System
NTEU	National Treasury Employees Union
NUPM	National Undercover Program Manager
NVWC	National Victim Witness Coordinator
OA	Office of Audit
OC	Oleoresin Capsicum
OCC	Office of Chief Counsel
OEO	Office of Enforcement Operations
OEP	Office of Employee Protection
OGE	Office of Government Ethics
OGE Form 202	Notification of Conflict of Interest Referral
OIA	Department of Justice Office of International Affairs
OIT	Office of Information Technology
OJI	On-the-Job Instructor
OJT	On-the-Job Training
OMS	Office of Mission Support
OPF	Official Personnel File
OPM	Office of Personnel Management

Abbreviation/Acronym	Meaning
OPR	Office of Professional Responsibility
OPS	Operations Division
Optional Form 26	Data Bearing Upon Scope of Employment of Motor Vehicle Operator
ORC	Operations Review Committee
ORI	Originating Agency Identifier
OSC	Office of Special Counsel
OSHA	Occupational Safety and Health Administration
PCA	Private Collection Agency
PDC	Private Debt Collection
PDT	Potentially Dangerous Taxpayer
PIF	Preparer Inventory File
PII	Personally Identifiable Information (PII)
POB	Place of Birth
POD	Post of Duty
PPM	Personal Property Manager
PROM	Pre-operational Meeting
QAM	Quality Assurance Manual
RFPA	Right to Financial Privacy Act of 1978, 12 U.S.C §§3401-3422
ROI	Report of Investigation

Abbreviation/Acronym	Meaning
RRA 98	Internal Revenue Service Restructuring and Reform Act of 1998 (Public Law 105-206)
SA	Special Agent
SSA	Senior Special Agent
SAAS	Security Audit and Analysis System
SAATP	Special Agent Advanced Training Program
SABT	Special Agent Basic Training
SAC	Special Agent in Charge
SAPTEP	Special Agent Part Time Employment Program
SAR	Suspicious Activity Report
SARC	Shooting and Assault Review Committee
SBSE	Small Business Self Employed
SCO	Systems Control Officer
SES	Senior Executive Service
SFD	South East Field Division
SIU	Special Investigations Unit
SISD	Special Investigations and Support Directorate
SSA	Social Security Administration
SSN	Social Security Number
S&W	Smith and Wesson

Abbreviation/Acronym	Meaning
TFSD	Technical and Firearms Support Division
TIG	Treasury Inspector General
TIGTA	Treasury Inspector General for Tax Administration
TIMIS	Treasury Integrated Management Information System
TSA	Transportation Security Administration
TSCM	Technical Surveillance and Countermeasures
TSO	Technical Services Officer
U.S.C.	United States Code
UC	Undercover
UCA	Undercover Agent
UNAX	Unauthorized Access
UPR	User Profile Records
US	United States
USA	United States Attorney
USAO	United States Attorney's Office
USMS	United States Marshals Service
USSS	United States Secret Service
VIN	Vehicle Identification Number
VRRA	Victims' Rights and Restitution Act

Abbreviation/Acronym	Meaning
VWPA	Victim and Witness Protection Act
WFD	Western Field Division
WTH	Work-to-Home

DATE: October 1, 2020

CHAPTER 400 – INVESTIGATIONS

(400)-10 Authority and Organization

10.1 Overview.
This Section contains information concerning the authority and organization of the Office of Investigations (OI).

- Authority
- Responsibilities
- Organizational Structure
- Statutes

10.1.1 Acronyms Table.

10.2 Authority.
The authority for the Treasury Inspector General for Tax Administration (TIGTA) is codified in the Inspector General Act (IG Act) and the Internal Revenue Service Restructuring and Reform Act of 1998 (RRA 98). Treasury Order 115-01, specifically item 2, "Audit and Investigative Matters," advises that in executing the functions of an Inspector General (IG), TIGTA is authorized to:

- Access return and return information, as defined in 26 U.S.C. § 6103(b), only in accordance with the provisions of 26 U.S.C. § 6103 and the IG Act;
- Access all facilities of the Internal Revenue Service (IRS) and Related Entities, including computer facilities and computer rooms, electronic data bases and files, electronic and paper records, reports and documents, and other material available to the IRS and Related Entities which relate to their programs and operations; and, when access is necessary to execute a function of TIGTA pertaining to a matter within the jurisdiction of TIGTA, all similar facilities throughout the Department;
- Make such investigations and reports relating to the administration of the programs and operations of the IRS and Related Entities that are, in the judgment of TIGTA, necessary or desirable;
- Request such information or assistance as may be necessary for carrying out the duties and responsibilities provided by the IG Act from any Federal, State, or local government agency or unit thereof;
- Require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary in the performance of functions assigned by the IG Act, which subpoena, in the case of contumacy or refusal to obey, shall be enforceable by order of any appropriate U.S. District Court: provided, that procedures other than subpoenas shall be used by TIGTA to obtain documents and information

from Federal agencies;

- Administer to or take from any person an oath, affirmation, or affidavit whenever necessary for the performance of TIGTA functions, which oath, affirmation, or affidavit when administered or taken by or before a TIGTA employee designated by TIGTA shall have the same force and effect as if administered or taken by or before an officer having a seal;
- Enforce criminal provisions of the internal revenue laws, other criminal provisions of law relating to internal revenue for the enforcement of which the Secretary is responsible, or any other law for which the Secretary has delegated investigative authority to the IRS pursuant to § 8D(k)(1)(A) of the IG Act. TIGTA and the Commissioner of the IRS (Commissioner) will establish policies and procedures to ensure that the TIGTA's and the Commissioner's responsibilities to investigate alleged offenses under the internal revenue laws and related statutes are delineated clearly;
- Carry firearms, and perform the following functions set out in 26 U.S.C. § 7608(b)(2):
  - Execute and serve search warrants and arrest warrants, and serve subpoenas and summonses issued under the authority of the United States;
  - Make arrests without warrant for any offense against the United States relating to the internal revenue laws committed in the TIGTA employee's presence, or for any felony cognizable under such laws if there are reasonable grounds to believe that the person to be arrested has committed or is committing any such felony; and
  - Make seizures of property subject to forfeiture under the internal revenue laws.
- Report any reasonable grounds believed to be a violation of Federal criminal law to the Attorney General of the United States in accordance with Sections 4(d) and 8D(k)(2) of the IG Act, subject to 26 U.S.C. § 6103;
- Investigate violations of 31 U.S.C. § 333 involving the misuse of the name or symbol of the IRS; the title of any IRS employee; the name or symbol of the Department of the Treasury in connection with internal revenue laws; or the title of any Treasury employee in connection with the activities of the IRS and Related Entities;
- Make determinations and issue orders, pursuant to 18 U.S.C. §§ 6001-6005, with the approval of the Attorney General, to compel the testimony under a grant of immunity of any individual who has been or may be called to testify or provide information at any proceeding before the IRS which such individual refuses to give or provide on the basis of the individual's privilege against self-incrimination; and
- Use the investigative, seizure and forfeiture authority under the Money Laundering and Control Act of 1986, 18 U.S.C. § 1956 and § 1957, where the underlying conduct is subject to investigation under the IG Act.

10.3 Responsibilities.
OI accomplishes its mission through proactive and reactive investigative programs that include investigations, operations, and studies. Generally, OI is responsible for:

- Investigating IRS employee misconduct involving violations of a criminal, civil or administrative nature;
- Investigating attempts by non-employees to corrupt or unlawfully interfere with the administration of the Federal tax system through such activities as bribery, threats or assaults, or other unlawful actions that may impact IRS personnel and impede Federal tax administration;
- Investigating actions by non-employees that may affect the safety of IRS employees or security of IRS facilities;
- Conducting armed escorts of IRS employees (See Section 260);
- Investigating non-employees who are involved in unauthorized disclosure or misuse of tax information;
- Investigating complaints against tax practitioners relating to the integrity of Federal tax administration (See Section 300);
- Conducting tort investigations of accidents involving TIGTA or IRS employees on official business (See Section 310);
- Investigating TIGTA employee misconduct involving violations of a criminal, civil or administrative nature;
- Conducting tests of high-risk integrity areas to detect corruption and other offenses involving IRS personnel and activities and alerting IRS management to potential integrity hazards and program vulnerabilities through information developed from these tests; and
- Responding to Congressional inquiries and conducting other special investigations.

10.4 Organizational Structure.
The Deputy Inspector General for Investigations (DIGI), who supervises investigative activities and inquiries relating to OI's programs and operations, leads OI. OI is separated into two functions:

- Special Investigations and Support Directorate (SISD); and
- Field Operations.

An Assistant Inspector General for Investigations (AIGI) leads each function with a Deputy Assistant Inspector General for Investigations (DAIGI) who assist the DIGI and are responsible for the supervision of specific Divisions that conduct investigative and support activities.

The DIGI may, notwithstanding other provisions of this chapter, assign any investigation to any Division or post-of-duty (POD) or waive any provision of policy stated in this Chapter at his/her discretion within the legal authority of TIGTA and the Treasury Use of Force policy.

Organizational charts are located on the TIGTA Intranet.

10.4.1 Special Investigations and Support Directorate. There are seven specialized or support divisions that comprise SISD:

- Criminal Intelligence and Counterterrorism Division (CICD);
- Cybercrime Investigations Division (CCID);
- Forensic and Digital Science Laboratory (FDSL);
- Fraud and Schemes Division (FSD);
- Operations Division (OPS);
- Special Investigations Unit (SIU); and
- Technical and Firearms Support Division (TFSD).

10.4.1.1 Criminal Intelligence and Counterterrorism Division. A Special Agent in Charge (SAC), who reports to the DAIGI-SISD, leads CICD. CICD provides OI Divisions with criminal intelligence and coordinates national collection and dissemination of criminal intelligence products.

10.4.1.2 Cybercrime Investigations Division. A SAC who reports to the DAIGI-SISD leads CCID. CCID is responsible for aggressively identifying and investigating electronic crimes or violations, which have the potential to compromise IRS networks and/or corruptly interfere with the IRS ability to conduct electronic tax administration, both internally and externally. CCID is comprised of three Groups:

- Network Investigations;
- Cyber Fraud; and
- Advanced Cyber Systems and Criminal Analysis.

10.4.1.2.1 Network Investigations. The Network Investigations Group is responsible for conducting investigations of attacks, intrusions, and threats delivered over/against the IRS and their computer systems, to include schemes to impersonate the IRS's online portals through advanced phishing campaigns and other sophisticated means. They also recommend effective countermeasures or actions to be taken by IRS system owners during a computer security incident investigation. In addition, they maintain the capability to respond to and perform analysis of computer systems involved in the administration of tax-related programs. They also work other Divisions and intelligence partners to mitigate or block emerging threats.

10.4.1.2.2 Cyber Fraud. The Cyber Fraud Group identifies and investigates misuses of IRS systems, primarily through external threats. They recommend preventative, recovery, or mitigation strategies for internal or external vulnerabilities or actual attacks. In addition, they work in consultation with other CCID Groups to develop methodologies to detect and respond to new or emerging schemes to defraud stemming from investigative or liaison efforts.

10.4.1.2.3 The Advanced Cyber Systems and Criminal Analysis. The Advanced Cyber Systems and Criminal Analysis Group is primarily responsible for identifying and developing new automated methodologies to detect unauthorized accesses to tax information within future-state IRS computer systems and perform advanced analytical support to various investigations.

10.4.1.3 Forensic and Digital Science Laboratory. A Director who reports to the DAIGI-SISD leads FDSL. FDSL performs the following functions:

- Provides forensic science expertise to support and develop case and mission related goals;
- Provides digital evidence collection and analysis in support of OI investigations;
- Conducts forensic analyses in the areas of questioned documents, latent prints, and digital evidence;
- Provide digital imaging, photography, and visual aids;
- Provide audio/video enhancements;
- Maintains liaison with other forensic laboratories for the purpose of technical information exchange and to support forensic analysis not conducted by the TIGTA's FDSL; and
- Conducts research and analysis relative to forensic and digital science, and develops and oversees training concerning these issues.

10.4.1.4 Fraud and Schemes Division. A SAC who reports to the DAIGI-SISD leads FSD. FSD continually evaluates domestic, national, or transnational criminal scheme activity to develop and share best investigative practices throughout OI. FSD is comprised of three Groups:

- Investigation Development
- Fraud Development; and
- Complaint Management Team.

10.4.1.4.1 Investigation Development. The Investigation Development Group is primarily responsible for the proactive detection and analysis of unauthorized accesses

(UNAX) to Federal tax information in IRS systems and fraudulent activity of IRS-generated Treasury checks (*e.g.,* altered, counterfeit, forged). The Group is also responsible for providing investigative analysis to special agents (SA), as needed, on complaints and investigations involving UNAX, misuse of data in Government equipment, contracts, and IRS refund check fraud.

10.4.1.4.2 Fraud Development. The Fraud Development Group is primarily responsible for conducting investigative initiatives involving national and transnational criminal scheme activity that did not originate through UNAX, misuse of data in Government equipment/contracts, or IRS refund check fraud. The Group is also responsible for providing investigative analysis to SAs, as needed, on complaints and investigations that did not originate through UNAX, misuse of data in Government/equipment/contracts, or IRS refund check fraud.

10.4.1.4.3 Complaint Management Team. The Complaint Management Team (CMT) is responsible for complaints management and records management. CMT is the central clearinghouse for complaints made to the TIGTA Hotline and is responsible for processing complaints received at TIGTA Headquarters.

CMT is responsible for organizational liaison with the IRS Employee Conduct and Compliance Office (ECCO), receiving, and accounting for complaints referred from the ECCO.

The Records Management Section (RMS) is located within CMT. RMS maintains all closed investigative case files and ensures they are maintained in compliance with Federal regulations and records retention schedules.

10.4.1.5 Operations Division. A SAC, who reports to the DAIGI-SISD, leads OPS. OPS is comprised of three Groups:

- Policy Team/Inspection Team;
- Statistics, Analysis, and Results Team; and
- Training Team.

10.4.1.5.1 Policy Team. The Policy Team supports the investigative operations of OI's headquarters and field divisions by providing oversight and guidance on policy matters. The Policy Team's responsibilities include:

- Researching, developing, and implementing national policy for OI;
- Administering OI national programs;
- Maintaining Chapter 400 of the TIGTA Operations Manual and OI forms;
- Responding to congressional inquiries;
- Preparing congressional testimony;

- Coordinating with TIGTA's Office of Chief Counsel on legal matters;
- Preparing briefing papers, speeches, and presentations on a variety of topics for OI executives;
- Preparing OI's narrative for the Semiannual Report to Congress;
- Providing input to TIGTA's annual IRS Major Management and Performance Challenges letter to the Secretary of the Treasury;
- Identifying significant investigative activity for weekly reporting to the Department of the Treasury;
- Preparing budget justifications and budget initiatives;
- Coordinating external reporting requirements;
- Notifying the IRS of indictments/criminal informations in unauthorized access/unauthorized disclosure investigations;
- Reporting conflict of interest referrals to the Office of Government Ethics;
- Processing Inspector General subpoenas, requests for cease and desist letters, and requests for authorization to use electronic equipment and consensual monitoring; and
- Administering OI's Intranet and Internet web pages; and
- Conducting Divisional inspections and CIGIE peer reviews.

10.4.1.5.2 Statistics, Analysis, and Results Team. The Statistics, Analysis, and Results Team is responsible for managing the Criminal Results Management System and analyzing production and performance data for internal and external reporting.

10.4.1.5.3 Training Team. The Training Team, located at the Federal Law Enforcement Training Center (FLETC) in Glynco, GA, serves as the focal point for assessing training needs and setting training objectives for OI. The Training Team's responsibilities include:

- Maintaining accreditation of the OI Training Academy;
- Providing technical assistance and support in the design, presentation, and evaluation of all OI training;
- Evaluating training conducted by field divisions;
- Maintaining liaison with the IRS-CI training component, as well as other Federal agencies, and professional law enforcement associations to keep abreast of new training developments;
- Collaborating with FLETC in the delivery of criminal investigator training;
- Providing technical assistance in developing training for other TIGTA and/or IRS employees;
- Promoting methods and means for maintaining OI's integrity awareness program; and
- Preparing presentation materials to professional groups; and
- Maintaining the Firearms, Agent Safety, and Tactics Program.

10.4.1.6 Special Investigations Unit. A SAC, who reports to the DAIGI-SISD, leads SIU. SIU investigates allegations of misconduct involving TIGTA personnel and certain IRS employees. SIU's responsibilities include:

- Conduct proactive and reactive investigations related to procurement integrity issues involving IRS employees, contractors, grantees, and other recipients of IRS funds;
- Reviewing allegations and conducting investigations involving Senior IRS officials at the GS-15 level and above (IR-1 and IR-3) and IRS-Criminal Investigation (CI) personnel;
- Reviewing and conducting investigations involving allegations concerning members of the IRS Oversight Board and IRS Office of Chief Counsel;
- Reviewing allegations and conducting investigations involving TIGTA employees, except for the Inspector General and certain other officials;
- Reviewing allegations and conducting investigations on other matters deemed sensitive, as directed by the DIGI; and
- Reviewing allegations and conducting investigations involving International (U.S. Competent Authority) employees located in Washington, D.C., and in U.S. embassies abroad.

In certain instances, other Divisions may conduct investigations into the above-mentioned matters with SIU oversight.

The DIGI may assign SIU to any investigation within the jurisdiction of TIGTA at his/her discretion.

10.4.1.7 Technical and Firearms Support Division. A SAC, who reports to the DAIGI-SISD, leads TFSD. TFSD has two components:

- Investigative Support; and
- Enforcement and Technical Operations.

10.4.1.7.1 Investigative Support. The Investigative Support Group is responsible for administering the following programs:

- Radio Communications Program;
- Integrated Wireless Network;
- Technical Surveillance Countermeasures;
- TECS; and
- Fleet Program.

10.4.1.7.2 Enforcement and Technical Operations. The Enforcement and Technical Operations Group provides technical investigative services to OI Divisions through Divisional Technical Agents.

10.4.2 Field Operations. Seven Divisions comprise Field Operations:

- Great Lakes Field Division (GLFD);
- Gulf States Field Division (GSFD);
- Mid-Atlantic Field Division (MAFD);
- Mountain Central Field Division (MAFD);
- North East Field Division (NEFD);
- South East Field Division (SEFD); and
- Western Field Division (WFD).

A SAC, who reports to the AIGI and DAIGI of Field Operations, leads each Division. Divisions are responsible for conducting investigations in assigned geographical areas and consists of PODs located throughout their geographical area. The seven Divisions and the States they cover are:

Field Division	States Covered:
Great Lakes	Illinois, Iowa, Indiana, Kentucky, Michigan, Minnesota, Missouri (Eastern), North Dakota, Ohio, South Dakota, and Wisconsin.
Gulf States	Arkansas, Louisiana, Mississippi, Oklahoma, and Texas.
Mid-Atlantic	Delaware, Maryland, New Jersey, Pennsylvania, Virginia, Washington, D.C., and West Virginia.
Mountain Central	Arizona, Colorado, Kansas, Missouri (Western) Montana, Nebraska, Nevada, New Mexico, Utah, and Wyoming.
North East	Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, and Vermont.
South East	Alabama, Florida, Georgia, North Carolina, South Carolina, Tennessee, Puerto Rico, and the U.S. Virgin Islands.
Western	Alaska, California, Hawaii, Idaho, Oregon, Washington, Guam, and the American Samoa Islands.

10.5 Statutes.

Statutes concerning most of the violations applicable to OI enforcement activities are listed in Exhibit (400)-10.1. This list does not mean that OI has primary jurisdiction for all of the listed statutes, rather intended as a guide in determining what statutes might be applicable to OI. Consult Titles 18, 26 and 31 of the U.S.C. for text, notes and other information.

CHAPTER 400 – INVESTIGATIONS

(400)-20 Responsibilities and Conduct

20.1 Overview.
All Office of Investigations (OI) employees must adhere to specific standards and policies in conducting their official duties. OI Special Agents (SAs) must possess and maintain the highest standards of conduct and ethics. SAs must also acquire and maintain certain knowledge, skills and abilities to carry out their investigative duties effectively.

This section contains information concerning the following:

- Employee Responsibility
- Investigative Responsibilities of Special Agents
- Standards for Ethical Conduct and Behavior
- Standards for Treasury Law Enforcement Officers
- Racial Profiling and Other Bias-Based Law Enforcement Actions
- Reporting TIGTA Employee Misconduct
- Lautenberg Amendment
- Requirement to Possess and Maintain Valid Driver's License
- Peace Officer Status and Scope of Employment
- Social Media

20.1.1 Acronyms Table.

20.2 Employee Responsibility.
Each OI employee is responsible for:

- Following the policies and procedures set forth in the TIGTA Operations Manual;
- Seeking guidance from management when confronted with unusual circumstances or questions about OI policy and procedure; and
- Contacting the Operations Division (*TIGTA Inv Operations) with questions concerning OI policies and procedures contained in Chapter 400 if management cannot resolve a question, or if an emergency, or a time sensitive/critical situation exists.

20.2.1 Certification of Review of Chapter 400. Each employee must review and certify each fiscal year that he/she is familiar with the contents of Chapter 400. This certification will be provided to the employee's first-line supervisor. See Exhibit (400)-20.1. Each supervisor will ensure that the certifications are updated by October 31st of

each year and will maintain these certifications in the employee's Employee Drop File for four years.

20.3 Investigative Responsibilities of Special Agents.
As a general rule, SAs are prohibited from taking any investigative steps unless a case or complaint has been initiated, numbered and assigned or otherwise approved by a supervisor. There are exceptions to this rule, including case development and authorized criminal intelligence-gathering activities that are approved by a supervisor.

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) has published the *Quality Standards for Investigations* (QSI), which provides a framework for conducting high-quality investigations for Offices of Inspector General affiliated with CIGIE. SAs shall be familiar with the CIGIE QSI, the principles of which are incorporated into the OI Operations Manual.

20.4 Standards for Ethical Conduct and Behavior.
Supervisors are to assure that employees are provided with the below listed information. Each employee is responsible for reading and understanding these documents:

- Standards of Ethical Conduct for Employees of the Executive Branch, U.S. Office of Government Ethics Standards, 5 C.F.R. Part 2635;
- Standards of Ethical Conduct for Employees of the Department of the Treasury, 5 C.F.R. Part 3101;
- Department of the Treasury Employee Rules of Conduct, 31 C.F.R. Subtitle A Part 0; and
- Office of Personnel Management Employee Responsibilities and Conduct, 5 C.F.R. Part 735.

Employees must observe and comply with all applicable standards of conduct established by appropriate authorities.

20.5 Standards for Treasury Law Enforcement Officers.
Treasury law enforcement officers (LEOs) must adhere to additional Treasury policies including:

- Policy on Off-Duty Conduct, Bias-Motivated Conduct, and Membership or Participation in Hate Groups by Law Enforcement Personnel;
- Giglio Policy; and
- Alcohol and Drug Policy.

20.5.1 Treasury Policy on LEO Off-Duty Conduct. On May 2, 1997, the Treasury Department issued a document titled, "Policy on Off-Duty Conduct, Bias-Motivated Conduct, and Membership or Participation in Hate Groups by Law Enforcement

Personnel," as part of the implementation process of the "Good O' Boys Roundup" Policy Review. TIGTA has adopted the Treasury Policy, which includes:

- **Off-Duty Conduct In General** – Treasury LEOs may be disciplined for violations of the rules governing employee conduct whether the violation occurs on or off duty, when violation of the rules adversely affects the efficiency of the Treasury Department, 31 C.F.R. Section 0.218. Treasury LEOs will not engage, on or off duty, in criminal, infamous, dishonest, or notoriously disgraceful conduct, or any other conduct prejudicial to the Government;

- **Bias-Motivated Conduct** – Treasury LEOs shall not use or engage in, on or off duty, abusive, derisive, profane, or demeaning statements, conduct, or gestures evidencing hatred or invidious prejudice to or about another person or group on account of race, color, religion, national origin, sex, sexual orientation, age, or disability. See 31 C.F.R. Section 0.217; and

- **Membership or Participation in Hate Groups** – Treasury LEOs who knowingly become or remain a member of or participate in a hate group or otherwise knowingly associate with the hate-motivated activities of others, proceed at the risk that their membership, participation, or association could reasonably be taken as tacit approval of the prejudice-related aspects of those groups or activities and could subject the officer to disciplinary investigation and possible disciplinary action. As used here, "hate group" or "hate-motivated activities" is defined as an organization, association, event, or activity, the sole or a primary purpose of which is to advocate or promote hate, violence, or invidious prejudice against individuals or groups on account of race, color, religion, national origin, sex, sexual orientation, age, or disability.

20.5.2 Giglio Policy. The Department of Treasury has adopted the Department of Justice's (DOJ) Giglio policy regarding the disclosure of potential impeachment information. OI employees who are potential witnesses in a Federal criminal case must inform the appropriate DOJ officials of any potential impeachment information as early as possible and prior to providing a sworn statement or testimony in any Federal criminal proceeding. Each potential witness should have a candid conversation with the Federal prosecutor regarding any on-duty or off-duty potential impeachment information including information that may be known to the public. See Chapter 700, Section 90.8.

20.5.3 Alcohol and Drug Policy. The Treasury Rules of Conduct prohibit the sale, use or possession of controlled substances and intoxicants by employees while on Departmental property, while on duty, or in a manner that adversely affects their work performance. See 31 C.F.R. § 0.204. TIGTA has the ability to conduct random drug testing of employees whose positions are characterized as sensitive (*e.g.*, employees who carry firearms, Presidential appointees requiring Senate confirmation, and personnel having access to sensitive information). SA positions are designated as

sensitive positions. See Chapter 600, Section 70.9, *Drug-Free Workplace Program*, for additional guidance regarding the program, and designated positions.
SAs may not use, or otherwise consume, any substance that may impair their ability to safely carry a firearm, operate a motor vehicle, or otherwise perform their law enforcement duties, at any time during their duty day, including law enforcement availability hours. See Section 180 of this Chapter for alcohol consumption related to undercover operations.

SAs temporarily assigned to any duty that does not require them to have access to a firearm or to a Government-owned vehicle (GOV) are held to the same standard as non-law enforcement employees, as described in the Treasury Rules of Conduct, 31 C.F.R. § 0.204, which prohibits employees from using, or consuming, substances or intoxicants in any manner which may adversely affect their work performance.
See Section 110 and Section 130 of this Chapter for further instructions concerning prohibitions on the use of substances and intoxicants while operating a GOV or using a firearm. Exceptions for SAs working in an undercover capacity are outlined in Section 180 of this Chapter.

20.6 Racial Profiling and Other Biased-Based Law Enforcement Actions.
SAs are prohibited from making decisions and/or taking law enforcement actions solely on the basis of race, color, national origin, ethnicity, gender, religion, sexual orientation, age, gender identity or disability. See 31 C.F.R. § 0.217.

20.6.1 Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity in Law Enforcement Actions. In December 2014, DOJ updated its *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity*. SAs are prohibited from invidious profiling and reliance upon generalized stereotypes based on a listed characteristic. Consistent with this guidance, agents should be guided by the following standards, in combination, when using race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity in law enforcement or intelligence activities:

- In making routine or spontaneous law enforcement decisions, such as ordinary traffic stops, Federal LEOs may not use race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity to any degree, except that officers may rely on the listed characteristics in a specific suspect description. This prohibition applies even where the use of a listed characteristic might otherwise be lawful.

- In conducting all activities other than routine or spontaneous law enforcement activities identified in the preceding bullet, which includes national security, homeland security and intelligence activities, Federal LEOs may consider race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity only to the extent that there is trustworthy information, relevant to the locality or

time frame, that links persons possessing a particular listed characteristic to an identified criminal incident, scheme, or organization, a threat to national or homeland security, a violation of Federal immigration law, or an authorized intelligence activity. In order to rely on a listed characteristic, including targeting communities possessing a listed characteristic, LEOs must also reasonably believe that the law enforcement, security, or intelligence activity to be undertaken is merited under the totality of the circumstances, such as any temporal exigency and the nature of any potential harm to be averted. This standard applies even where the use of a listed characteristic might otherwise be lawful. Additionally, LEOs may use a listed characteristic in connection with source recruitment, where such characteristic bears on the potential source's placement and access to information relevant to an identified criminal incident, scheme, or organization, a threat to national or homeland security, a violation of Federal immigration law, or an authorized intelligence activity.

These standards outlined above apply equally to State and local LEOs participating in Federal law enforcement task forces and at all times, including when Federal LEOs are operating in partnership with non-Federal law enforcement agencies. Federal LEOs are responsible for communicating these requirements, when applicable.

20.6.2 Use of Color, Age or Disability in Law Enforcement Actions. DOJ standards set forth in 20.6.1 of this section should also guide SAs in the use of color, age or disability as a basis for law enforcement actions and decision-making.

20.7 Reporting TIGTA Employee Misconduct.
The requirement to report misconduct to an appropriate authority is contained in the Department of the Treasury Employee Rules of Conduct, 31 C.F.R. Subtitle A Part 0. Any complaint, allegation, or information concerning misconduct by a TIGTA employee should be reported as explained in Chapter 200, Section 60 of the TIGTA Operations Manual.

20.7.1 Requirement to Report Arrests. If an SA is arrested, the SA will report the arrest to his or her immediate supervisor as soon as possible. The notification can be made verbally or in writing, and should include the following:

- Date of the arrest;
- The specific offense for which the arrest was made; and
- The name and address of the law enforcement agency making the arrest.

If available, a copy of the arrest report will be provided to the immediate supervisor by the employee.

The immediate supervisor will ensure that the information is promptly reported to the Special Investigations Unit for review. The immediate supervisor will also notify his/her Special Agent in Charge (SAC)/Director, who will notify their respective Assistant

Inspector General for Investigations or Deputy Assistant Inspector General for Investigations.

20.8 Lautenberg Amendment.
The Lautenberg Amendment, codified as 18 U.S.C. § 922(g)(9), prohibits anyone convicted of a misdemeanor crime of domestic violence from possessing firearms or ammunition, even in the line of duty. SAs who have been convicted of such a crime must notify their supervisor immediately. Refer all questions regarding the application of the Lautenberg Amendment to TIGTA Counsel for a determination.

20.9 Requirement to Possess and Maintain Valid Driver's License.
Because SAs may be required to drive a motor vehicle to perform law enforcement duties, each SA shall possess and maintain a valid driver's license from where the SA is domiciled in the United States or Puerto Rico. The immediate supervisor will ensure that each SA possesses and maintains a valid driver's license by reviewing each SA's driver's license at their mid-year and final performance appraisal reviews and will take corrective action against any SA who is not in compliance with the requirement.

See Section 110 of this Chapter for information on driver's license certification requirements when operating a GOV.

20.10 Peace Officer Status and Scope of Employment.
The Omnibus Consolidated and Emergency Supplemental Appropriations Act of 1999, P.L. 105-277, Div. A, Sec. 101(h), Title VI, Sec 627, provides that a Federal LEO shall be construed to be acting within the scope of his or her employment if the LEO takes reasonable action, including the use of force, to:

- Protect an individual in the presence of the LEO from a crime of violence;
- Provide immediate assistance to an individual who has suffered or who is threatened with bodily harm; or
- Prevent the escape of any individual who the LEO reasonably believes to have committed in the presence of the LEO a crime of violence.

Some States provide peace officer status to specific Federal officers, such as the Federal Bureau of Investigation or the Drug Enforcement Administration SAs, but do not give this status to all Federal LEOs. Research of State statutes revealed that the number of States that did not afford peace officer status to Federal LEOs far exceeded the number of States that extended peace officer status.

Unless covered by P.L. 105-277 or other applicable Federal law, actions taken solely under the authority of State law are beyond the authority of a Federal LEO's scope of employment.

In non-Federal crime situations, an SA's authority is that of a private citizen and the rules of "citizen arrest" apply.

20.10.1 Law As It Applies to OI Special Agents. An SA who acts as a peace officer under State law is not protected by the Federal Tort Claims Act and may be personally liable for negligent acts.

While a State may confer peace officer authority upon Federal LEOs, the State cannot broaden the jurisdictional limits of OI SAs established by Congress. A State may not impose a duty upon OI SAs to enforce State criminal laws.

20.10.2 Lawful Conduct – Peace Officer. The standards for determining whether certain conduct is lawful or unlawful are different for a peace officer and a private citizen.

A peace officer may make an arrest under different circumstances than those under which a private person may act. Generally, a peace officer may use greater force in effecting an arrest than a private citizen may use. Peace officers may be exempt from specific subsections of the State statute that make it unlawful to possess or carry certain weapons.

20.10.3 Liability When Acting as a Peace Officer. Unless an action is covered by P.L. 105-277 or other applicable Federal law:

- OI SAs may be held individually liable for damages absent State legislation or judicial decision affording indemnification under State law to peace officers.
- The U.S. Government may not be held liable for such actions nor may the Federal government indemnify Federal LEOs for damages assessed against them. TIGTA does not have the authority to pay any adverse judgment rendered against an employee acting outside the scope of his or her employment;
- A SA would not have the benefit of the qualified immunity afforded Federal employees acting within the scope of their employment and may not have the benefit of the defense of qualified immunity if their actions became the subject of litigation under 42 U.S.C. § 1983;
- Benefits may not be paid under the Federal Employees Compensation Act (FECA) to OI SAs who were injured as a result of actions taken in the capacity of peace officers; and
- The Department of Labor has discretion as to who will be eligible for benefits under the FECA.

20.11 Social Media.
Social media is a term used to describe internet or cellular phone-based applications and tools to share information among people. Social media includes networking websites, such as Facebook and Twitter, as well as bookmarking sites like Digg or Reddit.

20.11.1 Official Public Representation. Only official TIGTA spokespersons may speak on behalf TIGTA. Do not attempt to serve as a spokesperson through social media channels if you are not an official spokesperson. All media inquiries must be referred to the TIGTA Office of Communications (*TIGTA Communications). See Chapter 200, Section 90.

Do not use your TIGTA job title, official e-mail address or name of the IRS building where you work in your online interactions as it may give the false impression that you are speaking on behalf of the TIGTA or IRS. Public disclosure of your job title or employer - and its association with the IRS - may place you at a greater risk for internet and other security threats.

SAs are prohibited from using official U.S. Treasury, IRS, or TIGTA logos/emblems on their social media channels. SAs are prohibited from posting photographs of themselves where they can be identified as a TIGTA special agent, *e.g.*, wearing clothing that identifies them as a TIGTA special agent.

20.11.2 Official Business. Do not answer questions, or make statements about, or on behalf of TIGTA on a social network without explicit authorization. Social media channels are not the place to conduct confidential, official business with co-workers, subjects or stakeholders. The sharing of any official information via social media channels that could comprise the security of any law enforcement operation, TIGTA investigation or audit, or work facility is prohibited.

Do not post classified information, sensitive law enforcement information, or any other information if disclosure of that information would violate Internal Revenue Code Section 6103 or the Privacy Act.

20.11.3 Personal Use of Social Media. Do not openly associate yourself with TIGTA and do not promote your professional responsibilities in your profile(s) or posting(s) on social media websites. Do not provide details regarding your work colleagues, official position, duties, or training. Do not use your personal accounts to access social media sites for official business. See Chapter 200, Section 90.10.

Ensure all your posts and interactions are consistent with the public trust associated with your position and conform to existing standards outlined in *Plain Talk About Ethics and Conduct* and *Standards of Ethical Conduct for Employees of the Executive Branch* booklets.

CHAPTER 400 – INVESTIGATIONS

(400)-30 Managers' Responsibilities and Reporting Requirements

30.1 Overview.
This Section contains administrative instructions for Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations (OI) employees including:

- Division Certifications
- Annual Reports
- Quarterly Reports
- Case Management
- Review of Investigative Special Monies and Seized Property
- Reporting Significant Cases

30.1.1 Acronyms Table.

30.2 Division Certifications.
Each Special Agent in Charge (SAC)/Director (DIR) and Assistant Special Agent in Charge (ASAC)/Assistant Director (AD) is responsible for managing TIGTA's investigative and administrative activities within their operational area. See Exhibit(400)-30.1 for a listing of Management Authorities and Delegations.

As applicable, each SAC/DIR will conduct reviews of operational activities of all ASACs/ADs and all associated posts of duty (POD) in their division. Each SAC/DIR will certify the completion of and report on the findings of these reviews according to the certification schedule listed in Exhibit(400)-30.2.

The ASAC/AD will conduct the Division Certifications review for their respective group, identifying the specific issues and any corrective measures taken, if necessary. Each SAC/DIR will certify each Divisional Certification for their division and also identify and certify that completed corrective measures, as applicable.

SACs/DIRs are required to complete seven Division Certifications annually. Certifications are due on the last day of the month indicated, outlined below:

- **January** – Accountable Properties: Annual certification regarding inventory of identification, fleet records, and travel cards;
- **February** – Confidential Sources and Fictitious Identities: Annual certification of policy compliance regarding review and control of confidential sources and fictitious identities;

- **April** – Case and Program Management: Annual certification of case timeliness, undercover operations, grand jury procedures, blanket declination agreements, and agency's goals;
- **June** – Space and Physical Security: Annual certification of physical security review of Divisional offices, including all PODs within the Division;
- **August** – Evidence and Seized Properties: Annual certification of policy compliance regarding evidence processing and storage;
- **October** – Training: Annual certification of training completion regarding firearms, control tactics, vehicles, and travel cards; and
- **November** – Resource Management: Annual certification of employee staffing, personnel files, professional development, Equal Employment Opportunity, and Operations Manual review.

In circumstances where the last day of the month falls on a weekend, the Division Certification must be uploaded on the next business day. SACs/DIRs must submit all Division Certifications and respond to all questions. Any questions not relevant should be marked "N/A."

The certifications are located on the Division Certifications SharePoint site under the "MASTER Certification Documents" tab.

30.3 Annual Reports.
The following reports must be prepared annually and forwarded as indicated. Report due dates are included in Exhibit (400)-30.2.

30.3.1 Requests for New Equipment. Requests for new equipment will be made by the DFCs.

30.3.2 Ammunition Inventory Report. For further information see Section 130 of this Chapter.

30.3.3 Annual Certification of Law Enforcement Availability Pay Hours. For further information, see Section 40.3 of this Chapter.

30.3.4 Annual Social Security Number and Fictitious Identity Package Reviews. For further information, see Sections ******** and ********** of this Chapter.

30.3.5 Annual Report on Physical Security of TIGTA Offices. Each SAC/DIR will conduct a physical security review of all PODs within the division on an annual basis. Certifications are due annually by June 30th.

30.4 Quarterly Reports.
The following reports must be prepared quarterly:

- PPM updates to the TIGTA Office of Mission Support (OMS) are due by the 3rd of each month following the end of each quarter;* and
- Investigative Imprest Fund report due by the 10th of each month following the end of each quarter.

*TIGTA Forms OI 141, *Statements of Special Money and Property Transaction*, are required to be submitted within five business days of the property acquisition, and are in addition to quarterly reporting requirements.

Quarterly report due dates are outlined in Exhibit (400)-30.2.

30.4.1 Performance and Results Information System Property Module Update to the Office of Mission Support. For further information, See Chapter 600, Section 50.11.6.1.

30.4.2 Review of Investigative Imprest Fund. SACs/DIRs will conduct quarterly unannounced reviews of their investigative imprest funds. This review should consist of an unscheduled cash verification of the imprest fund at least once each calendar quarter. Refer to Chapter 600, Section 50.9.8.1 for guidance. These reviews determine if controls are adequate for proper accountability, maintenance, and security.

The SAC/DIR determines if:

- The fund is being used only for the purposes established;
- Fund advances and expenditures are properly authorized and approved.
- The fund is maintained at the lowest practical level;
- Accountability reports are accurate and submitted on a timely basis, and any losses from the fund are properly documented and reported to the Bureau of the Fiscal Service;
- Proper accounting methods are used for expenditures to or on behalf of informants, prescribed rules are followed for payment involving information gathering and informants, and evidence verifies the existence of paid informants;
- Expenditures are appropriate and reasonable under the circumstances, and are effectively used to develop the related investigation;
- Information or services provided by paid informants could not have been obtained through more practical means, such as Internal Revenue Service (IRS) or third-party records;
- Physical and internal controls are effective to protect the fund and supporting documents; and
- Established physical safeguards are working effectively to protect the identity of confidential informants.

Document the review including the results of the cash verification, in a memorandum to the appropriate AIGI by the 10th of January, April, July, and October each year. A copy of the memorandum must be saved in the respective division's subdirectory on the Division Certifications SharePoint site.

30.5 Case Management.
Effective case management is necessary to ensure timely investigation and referrals for administrative or prosecutive actions. Investigations must be thorough and timely to avoid:

- The inability to take administrative actions due to the untimely submission of reports; or
- A prosecution being declined or made impossible due to an elapsed statute of limitations.

Refer to the Case and Program Management Certification for specific guidance on areas of review.

30.5.1 Use of Investigative Resources. ASACs/ADs and special agents (SA) are jointly responsible for ensuring that investigative resources are used effectively. To do so, they must consider whether a matter is actionable at the initiation of the case and during periodic reviews. See Section 240 of this chapter for additional guidance on initiating investigations. SAs will document any formal prosecutive opinion in TIGTA Form OI 2028R, *Report of Investigation*.

30.5.2 Evaluating Information in Leads, Intakes, and Investigations. SACs/DIRs are responsible for ensuring that investigations relate to TIGTA's mission.

ASACs/ADs must evaluate all information, solicited or unsolicited, to ensure that the information is:

- Within TIGTA's investigative jurisdiction; and

Processed in accordance with the Privacy Act of 1974. See Section 210 of this Chapter, for additional information.

ASACs/ADs may authorize the initiation of all investigations except for the following two types of investigations that require a higher level of approval as listed below:

- Sexual Harassment Investigations: Requires concurrence from the SAC/DIR-Division, to initiate the investigation, or the SAC-Special Investigations Unit (SIU) to initiate the investigation for subjects under SIU's investigative purview; and

- Non-employee Investigations involving Counterterrorism allegations: Requires the SAC of the division's approval and notification of the SAC-Criminal Intelligence and Counterterrorism Division to initiate these investigations.

30.5.3 Allegations Concerning Internal Revenue Service Employees. ASACs/ADs must evaluate all allegations of misconduct against IRS employees, and within 30 calendar days of receipt of the information, they must:

- Open an employee investigation; or
- Refer the matter to IRS management; or
- Refer the matter to another agency; or
- Close the intake to file if no action is warranted.

See Section 240 concerning complaint processing.

30.5.4 Referrals to Other Federal, State and Local Authorities. Investigations may uncover violations that are not within TIGTA's jurisdiction. Refer these matters to the Federal, State, or local agency that has investigative or prosecutive authority. Before making referrals to agencies outside of the IRS consult Chapter 700, Section 70.5 of the TIGTA Operations Manual for the proper procedures.

30.5.5 Case Reviews. ASACs/ADs must conduct case reviews as follows:

- At least every 90 days;
- On all open investigations in their respective groups;
- Applying the guidelines set forth in Section 20.3 of this Chapter; and
- Stressing the necessity for timely completion of investigations.

During each case review, the ASAC/AD will:

- Review the case file and the TIGTA Form OI 6501, *Chronological Case Worksheet*;
- Discuss the case with the SA/analyst; and
- Make an entry on TIGTA Form OI 6501 entitled "Case Review," the date of review, the ASAC's/AD's initials, and a notation of significant matters discussed related to the progress of the investigation (*e.g.*, priorities, leads to be pursued).

While every investigation is unique, topics typically discussed during a case review include:

- The scheduling of upcoming interviews;

- The use of technical and forensic support available from the Fraud and Schemes Division , the Forensic and Digital Science Laboratory and TFSD;
- The use of the Undercover Program;
- Evidence collection, chain of custody, and storage;
- Grand jury involvement and protection of grand jury information;
- Elements of the offense proven or unproven;
- Solvability factors;
- Criminal Results Management System accuracy;
- The estimated date of completion, commonly referred to as the "EDC" for the investigation;
- Utilization of electronic processes and techniques; and
- Current OI Program Guidance.

30.5.6 Timeliness of Investigations. Criminal investigations may extend beyond 365 days when the two conditions below are met:

- The case agent has documented a discussion with an Assistant United States Attorney (AUSA) who has either accepted an investigation for prosecution, or has committed to pursuing prosecution if specific, articulable investigative leads result in sufficient evidence to prove the elements of the offense. The discussion with the AUSA does not have to be a formal referral; however, it must be documented on TIGTA Form OI 6501, including any additional investigative leads needed to complete the investigation; and
- The SAC/DIR concurs that there is investigative potential to justify extending the investigation beyond 365 days. The SAC/DIR must document their extension approval on TIGTA Form OI 6501, and conduct annual reviews and approvals of the extension thereafter. SAC/DIR extension authorizations do not supersede the requirement for timely case reviews outlined in Section 250.

When an investigation is required to remain open for more than three years, approval from an AIGI or a Deputy AIGI (DAIGI) is required. The AIGI or DAIGI's approval must be recorded on TIGTA Form OI 6501.

The requirement to complete administrative investigations within 120 days will also be extended if the case involves serious administrative misconduct related to an IRS employee post appointment arrest (PAA) and the results of that PAA will have an impact on the IRS employee's ability to perform their duties.

30.5.7 Supervision of Special Agents. SAs at the journey level (GS-13) and above generally receive more autonomy. However, ASACs/ADs will review their decisions to ensure diligence in completing assignments and that person hours are not wasted

through over-investigation. Successful performance at this level requires SAs, for the most part, to independently:

- Plan and conduct investigations which resolve the issues involved;
- Determine the sequence and timing of investigative efforts;
- Accurately appraise findings; and
- Determine whether further leads are warranted.

30.6 Review of Investigative Special Monies and Seized Property.
The SAC/DIR ensures that annual reviews are conducted of investigative special moneys and seized property. These reviews determine if controls are adequate for:

- Proper accountability;
- Maintenance and security; and
- Timely and adequate disposition.

SACs/DIRs are responsible for the following:

- Discussing controls and security over the funds and property with the appropriate evidence custodian and Divisional PPM Coordinator;
- Ensuring that a physical inventory is conducted of all evidence currently maintained by the POD's under review;
- Ensuring the results of the physical inventory are compared to the evidence log;
- Ensuring TIGTA Forms OI 141 for the review period are compared with the evidence log to determine whether acquisitions and dispositions of seized property are properly and timely prepared;
- Determining if TIGTA requirements for security measures are met;
- Discussing with the ASACs/ADs their method for emphasizing the need for SAs to report and account for special moneys and seized property; and
- Reviewing documentation on the disposal of narcotics performed during the review period to determine whether the disposal was witnessed by two SAs.

Refer to the Evidence and Seized Property Certification for specific guidance on areas of review. See Section 30.2 for certification information and location.

30.7 Reporting Significant Cases.
SACs/DIRs are responsible for ensuring familiarity with investigations in their division and for recognizing cases and events that may have a significant impact on the Department of the Treasury, the IRS, or TIGTA. TIGTA Form OI 2020, *Fact Sheet*, is required to report investigations resulting in administrative and/or judicial action or other significant action. Examples of activities that require a TIGTA Form 2020 include:

- Investigations with likely widespread media interest, congressional interest, or with the potential for notoriety or significant impact on the IRS, the Department of the Treasury, or TIGTA;
- Arrests made by TIGTA SAs, including when and where the initial appearance was held;
- Search warrants including other agency search warrants in which TIGTA participated;
- Judicial actions including any indictment, information, pre-trial diversion, verdict, pleading, sentencing or any declination of significant impact;
- Any threat of, or actual, serious violence directed against IRS or TIGTA employees or property;
- Any actions by IRS or TIGTA personnel causing injury or loss of life;
- Any discharge of firearms by IRS or TIGTA personnel, other than training-related, on or off duty;
- Any employee investigation resulting in noteworthy administrative action;
- Any employee investigation that may warrant the IRS Commissioner's immediate attention; or
- Any investigation involving significant mismanagement matters, including misuse of enforcement and production statistics.

30.7.1 Completion of TIGTA Form OI 2020. Complete Forms OI 2020 forthwith, generally within 24 hours following the event of significant impact.

30.7.2 Submission of TIGTA Form OI 2020. The SAC/DIR is responsible for reviewing, approving, signing, and submitting TIGTA Forms OI 2020. Upon SAC/DIR approval, upload TIGTA Forms OI 2020 to the Fact Sheet SharePoint site for review and approval by the appropriate Deputy AIGI (DAIGI) or AIGI, as appropriate. If exigent circumstances necessitate immediate notification, the SAC/DIR must contact the appropriate AIGI or DAIGI and follow up with the submission of TIGTA Form OI 2020 within 24 hours.

30.7.3 Distribution of TIGTA Forms OI 2020. The Operations Division retains TIGTA Forms OI 2020 and distributes copies to senior TIGTA management, as required. Additionally, TIGTA Forms OI 2020 are available to OI personnel through the Fact Sheet SharePoint site.

DATE: July 1, 2019

CHAPTER 400 – INVESTIGATIONS

(400)-40 General Information

40.1 Overview.
This section contains the following general information for the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations (OI) employees:

- Chapter 400 of the TIGTA Operations Manual
- Law Enforcement Availability Pay
- Accommodations for Agents with Temporary Medical Conditions
- Acknowledgements for Cooperating Internal Revenue Service (IRS) Employees
- Outside Employment or Activity
- Office of Preference Program
- Collateral Duties

40.1.1 Acronyms Table.

40.2 Chapter 400 of the TIGTA Operations Manual.
Chapter 400 of the TIGTA Operations Manual provides guidance on policies and procedures specific to OI. OI personnel should consider the entire Operations Manual when seeking guidance on investigative matters, because relevant information may be found in other chapters. OI personnel must seek supervisory guidance if confronted with a situation not addressed by the Operations Manual. The Operations Manual is solely for internal guidance. It does not place any limitations on otherwise lawful investigative or litigative prerogatives of TIGTA.

Chapter 400 will be updated, when necessary, to reflect new policies and procedures. Each update will contain a corresponding manual transmittal outlining the changes. See Chapter 100, Section 70.3.2.

Policy questions or suggestions should be directed to the Operations Division via e-mail to *TIGTA Inv Operations.

40.2.1 Accessibility. The Operations Manual is accessible by all TIGTA personnel, and a redacted version of the Operations Manual is available to the public via the TIGTA Internet page.

The Deputy Inspector General for Investigations (DIGI) has the authority to issue periodic interim guidance to OI employees, based on the needs of the Agency. Interim guidance remains in effect until it is either codified into the appropriate manual chapter or rescinded. See Chapter 100, Section 100.

40.2.2 Personnel Title References. Currently, OI's investigative staff consists of:

- Criminal Investigators/Special Agents (SAs) - GS-1811
- Investigative Specialists - GS-1801
- Investigative Analysts – GS-1805

In Chapter 400, "investigator" refers to SAs (series GS-1811) and investigative specialists (series GS-1801). When "SA" or "agent" is used, it refers only to series GS-1811s and is used in the context of responsibilities of, or actions taken only by, criminal investigators.

40.3 Law Enforcement Availability Pay (LEAP).
The LEAP Act of 1994, 5 U.S.C. §§ 5542(d) and 5545a, authorizes the payment of 25% of basic pay to criminal investigators to ensure their availability for unscheduled duty in excess of their 40-hour basic workweek. LEAP is considered part of basic pay for the computation of retirement benefits, lump sum annual leave, life insurance, and, where applicable, the value of subsistence and quarters.

40.3.1 Definitions. Several terms have specific meanings when used in the context of LEAP, including the following:

- "Availability" means that, an SA is either performing official duties during unscheduled duty hours or is generally and reasonably accessible by TIGTA to perform official duties during unscheduled duty hours;
- "Unscheduled duty hours" are hours an SA works or is available to work that are not part of the 40-hour basic work week or not regularly scheduled overtime hours;
- "Administrative work week," for OI, is the period of seven consecutive days beginning Sunday and ending the following Saturday;
- "Basic work week" for full-time employees, means a 40-hour work week;
- "Regular work day" is each day in the basic work week during which an SA works at least four hours that are not regularly scheduled overtime hours or unscheduled duty hours; and
- "Excludable day" is any day on which an SA took more than four hours of approved leave, received more than four hours of training, was on official travel status for more than four hours, did not work due to an official Federal holiday, or was excused from work for job relocation purposes.

Note: Days in leave without pay status are not considered to be regular work days for the purpose of LEAP and are not considered in determining whether an SA has met the annual LEAP requirements.

40.3.2 Eligibility for Availability Pay. All SAs (grades 5 through 15) are eligible to receive LEAP. Before being placed on LEAP, SAs must certify they expect to meet the minimum requirements to receive LEAP during the fiscal year and, if applicable, that they met the requirements for the prior year. See Exhibit (400)-40.1 for the certification form. SAs must certify, in writing, by October 10 of each fiscal year that they expect to continue to meet those requirements. The certification form must be provided to the SA's immediate supervisor.

SAs continue to be eligible for LEAP even when they cannot reasonably and generally be accessible due to a status or assignment approved or ordered by OI, including:

- Relocation;
- Travel;
- Annual leave;
- Sick leave; and
- Training (See Section 40.3.5.3).

40.3.3 Temporary Exemption from Certification. Some SAs may not be able to perform official duties during unscheduled duty hours to the extent required to receive LEAP. SAs may apply for a temporary exemption from certification for a determined period of time if compliance with LEAP requirements creates a hardship. The application for exemption is part of the certification form shown in Exhibit (400)-40.1. At any time during the fiscal year, the SA may complete the LEAP certification and apply for an exemption. SAs voluntarily participating in the SA Part-time Employment Program should refer to Exhibit (400)-40.4.

40.3.4 Requirements for Availability Pay. SAs must certify that, over the course of the fiscal year, they were available to work an average of at least two hours per day, which were:

- Unscheduled duty hours worked on a regular work day;
- Unscheduled duty hours worked on a non-regular work day; or
- Unscheduled duty hours an SA is available to work on a regular work day at the direction of management.

Note: Management requests for availability must be assignment-specific and not a blanket open-ended request.

40.3.5 Calculating LEAP Hours. Hours an SA spends in an available status may or may not be included as qualifying hours for LEAP calculation, depending upon whether it occurs on a regular work day or a non-regular work day.

40.3.5.1 Regular Work Day. If the SA is available on a regular work day, the LEAP calculation includes any hours actually worked or in available status. If the SA is available on a non-regular work day, the LEAP calculation includes only the hours actually worked.

40.3.5.2 Temporary Assignments. Temporary assignments that include providing training may be claimed as excludable days, since these duties are agency-directed assignments. However, any hours worked by an SA preparing or providing training beyond the normal eight-hour day may be considered unscheduled duty hours.

40.3.5.3 Training Status. SAs may claim LEAP hours while in overnight training status (*e.g.*, FLETC) when the SA performs actual work in excess of the eight-hour training day. For instance, the SA may use the gym and claim LEAP under Health Improvement Program (HIP) activities or engage in intake or investigative activities by writing reports or reviewing documents.

40.3.6 Effect of Availability Pay on Other Compensation. SAs who certify that they expect to meet the requirements to receive LEAP are exempt from the Fair Labor Standards Act of 1938.

SAs may receive overtime pay only for work in excess of the normal eight-hour work day, which was scheduled in advance of the administrative work week. Even so, the first two hours of the scheduled work are counted as LEAP hours. Scheduled work in excess of those two hours is reported and compensated as overtime. SAs normally will not be assigned regularly scheduled overtime.

There is no upper limit to the amount of unscheduled duty hours an SA may work in a fiscal year. SAs cannot be compensated, either by pay or compensatory time off, for unscheduled duty hours worked over the annual daily average requirement.

40.3.7 Documentation for Availability Pay. SAs must accurately record unscheduled duty hours available or worked for annual LEAP calculation purposes in their Criminal Results Management System (CRIMES) time report.

Supervisors must review and certify LEAP hours documented in CRIMES to ensure accuracy and that SAs are meeting LEAP requirements.

40.3.8 Request for Availability Pay. After an SA certifies that he/she has met the LEAP requirements for the prior year and expects to meet the requirements to receive LEAP for the current fiscal year, the immediate supervisor notifies, in writing, the Special Agent in Charge (SAC) or the respective Deputy Assistant Inspector General for Investigations (DAIGI) or Assistant Inspector General for Investigations (AIGI). This memorandum authorizes payment of LEAP to the SA. See Exhibit (400)-40.2 for a sample notification memorandum.

40.3.9 Quarterly Availability Hours Review. Immediate supervisors must conduct quarterly reviews to ensure that SAs remain qualified for LEAP. If the review reflects that an SA did not meet the required daily two-hour average of unscheduled duty or availability, the immediate supervisor will advise the SA, in writing (via e-mail or memorandum), that he/she is in danger of not meeting the annual qualification requirements for LEAP. The immediate supervisor and the SA are responsible for establishing a course of action to enable the SA to meet the annual requirement.

Immediate supervisors must document in a memorandum any quarterly review revealing that an SA is below the daily two-hour average. This memorandum will be forwarded to the SA's second-level supervisor. The memorandum will include the following information:

- Circumstances for not meeting the LEAP requirement; and
- Corrective action planned.

Immediate supervisors will forward the documentation to the second-level supervisor or the respective DAIGI or AIGI.

40.3.10 Annual Certification of Availability. At the end of each fiscal year:

- All immediate supervisors conduct an annual review and certification of qualification for LEAP, specifying that the SAs have met and are expected to continue to meet LEAP requirements; and
- Each SAC/Director will report the results to the appropriate DAIGI/AIGI by October 20, of each fiscal year. See Exhibit (400)-40.3 for a sample format.

40.3.11 Removal from Availability Pay. SAs who do not meet the annual hourly average requirement will be removed from LEAP. Removal from LEAP is considered an adverse personnel action and must be processed accordingly.

40.3.12 Administratively Uncontrolled Overtime. Employees who are not covered by LEAP may be eligible to receive administratively uncontrolled overtime (AUO). See Chapter 600, Section 70.4.6.2.

40.4 Accommodations for Agents with Temporary Disabling Medical Conditions. OI will make reasonable efforts to accommodate and support SAs with temporary disabling medical conditions. To the maximum degree possible, these SAs will be allowed to continue their normal duties.

40.4.1 Temporary Disabling Medical Condition Defined. A "temporary disabling medical condition" is a non-permanent medical condition that:

- Incapacitates the SA for a limited period of time but not more than 12 months; and
- Limits the range or duration of activities the SA can fully and safely perform for a limited period of time but not more than 12 months.

For the purpose of this policy, pregnancy is considered a temporary disabling medical condition. However, due to the unique nature of pregnancy, several additional factors apply. See Section 40.4.4 for guidance related to pregnant SAs.

40.4.2 Employee Responsibilities. SAs must notify their immediate supervisor as soon as a temporary disabling medical condition is diagnosed. The SA must submit a statement from a licensed physician verifying the condition and identifying activities that he/she cannot perform. The SA will submit an updated statement from a physician to his/her immediate supervisor every two months.

40.4.3 Supervisor Responsibilities. Supervisors may not require SAs with temporary disabling medical conditions to perform certain duties, such as qualifying with a firearm or making an arrest, when engaging in those activities could reasonably be expected to either:

- Place the SA or others in unnecessary danger; or
- Exceed the physical capabilities of the SA.

Supervisors must document any modifications made to an SA's duties based on this policy. A supervisor may not deny an employee's request to modify his/her duties due to a temporary disabling medical condition without first obtaining guidance from TIGTA's Office of Chief Counsel.

Note: Medical documentation received from an employee (*e.g.,* a physician's statement concerning a temporary disabling medication condition) should be maintained in a confidential file separate from any other personnel file and clearly marked as "medical confidential." This documentation should not be maintained in an employee's performance file or drop file. It is recommended that the medical documentation be sealed (*e.g.,* in an envelope clearly marked as "medical confidential"). Additionally, confidential medical documentation should be appropriately secured (*e.g.,* in a locked cabinet, drawer, or office), and access to this information limited only to those individuals whose official duties require such access. In the event that medical documentation is received by a supervisor via e-mail, the documentation should be printed, maintained as described above, and the incoming e-mail should be deleted.

Questions regarding the proper handling of medical information should be directed to TIGTA's Office of Chief Counsel or TIGTA's Equal Employment Opportunity Program Manager.

40.4.4 Accommodations for Pregnant SAs. A pregnant SA should consult her physician regarding:

- What activities she should or should not perform; and
- Possible firearms range hazards, such as lead exposure and gunshot noise.

A pregnant SA may decide whether or not to continue firearms qualification during her pregnancy. Regardless of her decision, she must provide documentation from her physician supporting her decision, and provide updated documentation from her physician every two months.

Pregnant SAs are authorized to qualify with, but not carry, non-standard lead-free ammunition, if available. Firearms instructors should ensure that the performance of the non-standard ammunition closely approximates that of standard duty ammunition.

40.4.5 Firearms Carry. Regardless of medical condition, SAs will not carry a firearm if their firearms qualification is not current and the SA does not have a waiver. See Section 130.4.2.2, *Temporary Waiver from Firearms Qualification*. An SA who cannot carry a firearm will not knowingly be placed into or allowed to enter into situations where a firearm is reasonably likely to be needed.

40.5 Acknowledgements for Cooperating IRS Employees.
TIGTA acknowledges IRS employees for significant contributions to its mission through letters of commendation. TIGTA does not recommend or give monetary awards to cooperating IRS employees. TIGTA may give acknowledgements for any matter in which an employee has cooperated with TIGTA.

40.5.1 Letters of Commendation. The Inspector General may sign Letters of Commendation for IRS employees who assist TIGTA in the successful completion of investigations.

When preparing Letters of Commendation for the Inspector General's signature:

- Prepare the letter for his/her signature;
- Prepare a brief transmittal memorandum to the IRS Commissioner from the Inspector General; and
- Submit the original letter and the transmittal memorandum to the DIGI.

40.6 Outside Employment or Activity.
TIGTA does not have a specific blanket policy regarding the prohibition or approval of outside employment or activity. Instead, each request for outside employment or activity will be considered and acted upon separately. TIGTA's Office of Chief Counsel is responsible for final determinations regarding whether a request presents an actual, potential, or apparent conflict of interest. See Chapter 700, Section 30.3.

40.6.1 Evaluating Outside Employment or Activity Requests. There are several, often interdependent, contexts in which TIGTA reviews requests to engage in outside employment or an outside activity. Key factors considered include workload management, operational concerns or needs, and the potential for, appearance of, or existence of, a conflict of interest under Federal ethics laws and regulations. The first and second-level supervisors are responsible for evaluating requests for workload or operational considerations. The appropriate DAIGI/AIGI is responsible for approving the request.

TIGTA's Office of Chief Counsel will review all DAIGI/AIGI-approved requests to engage in outside employment or outside activity for the potential appearance or existence of a conflict of interest or other disqualifying ethical issues or concerns.

40.6.1.1 Work Hours and LEAP. SAs approved for outside employment or outside activities who are receiving LEAP must be available for unscheduled duty. Any management directive for the SA to report for duty for a specific assignment preempts any outside employment or activity approval. Failure to report as directed may result in disciplinary or adverse action.

40.6.1.2 Work Assignments. All SAs receiving LEAP will continue to be assigned case and administrative work regardless of any engagement in outside employment or activity. Directed assignments, including temporary duty, detail assignments and task force operations, shall not be adversely impacted by outside employment or activities.

40.6.1.3 Ethical Considerations and Conflict. SAs may not engage in any outside employment or activity that gives rise to a real, potential, or perceived conflict of interest. Such activities may include, but are not limited to:

- Legal employment or tax practice – legal activities involving Federal, State, or local tax matters or any matter in which the United States is a party, to include accounting; appearance on behalf of taxpayers, bookkeeping, or preparation of tax returns for compensation;
- General investigative work – performing as a private investigator, background investigator, conducting insurance claim inquiries, special police or security guard; and
- Law enforcement officer – member of a State or local law enforcement organization as a reserve or auxiliary officer where State or local law enforcement authorities are exercised.

OI employees may not engage in any outside employment or activity that might bring discredit upon or lower public confidence in TIGTA, the Department of the Treasury, or the U.S. Government, in general.

40.6.2 Submitting Outside Employment or Activity Requests. OI employees may request approval to engage in outside employment or activity by:

- Completing Form 7995, *Outside Employment or Business Activity Request*; and
- Completing a supplemental statement, if requested by TIGTA management.

Requests for outside employment or activities will be processed as follows:

- The employee will submit a properly completed written request for consideration via Form 7995 to his/her immediate supervisor;
- OI management must make a final decision on the request to engage in outside employment or activity as soon as possible, but no later than 10 workdays from receipt of the fully completed request. Upon receipt, the immediate supervisor will evaluate the request based on local workload issues and operational considerations and will forward the Form 7995 with his/her written recommendation to the second level supervisor for preliminary consideration;
- The second level supervisor will review and forward the entire package, including his/her written recommendation for disposition of the request, to the appropriate DAIGI/AIGI for determination;
- If the DAIGI/AIGI denies the request, a memorandum will be sent to the OI employee that explains the specific reason(s) for the denial, no later than 10 workdays from management's initial receipt of the fully completed request;
- If the DAIGI/AIGI approves the request, the entire package will be sent forward to TIGTA's Office of Chief Counsel for review;
- A memorandum is sent to the OI employee for all requests returned by TIGTA's Office of Chief Counsel. If denied due to an ethics determination, a complete explanation is to be provided to the OI employee; and
- TIGTA's Office of Chief Counsel is to review all DAIGI/AIGI-approved applications for the potential, appearance, or existence of a conflict of interest or other disqualifying ethical issues or concerns. TIGTA's Office of Chief Counsel will notify the DAIGI/AIGI of the ethics determination, no later than 15 workdays from their receipt of the request. All denials will include a written explanation.

A copy of all supporting documents used in making the determination regarding participation in outside employment or outside activities shall be retained by the employee's immediate supervisor in the employee's drop file. The respective DAIGI/AIGI shall retain the originals of all supporting documents for a one-year period.

An approval to engage in outside employment or activity will be for a specified period not to exceed the end of the calendar year. OI employees must reapply for outside

employment or outside activity prior to the end of each calendar year. In addition, if during the year the employee changes position/status, or when the conditions of outside employment change, OI employees must reapply for approval for the outside employment or activity.

40.6.3 Activities That Do Not Require Prior Approval. TIGTA Operations Manual Chapter 700, Section 30.3 lists activities that do not require prior TIGTA approval under this guidance. OI employees with questions or concerns relating to outside employment or outside activity should contact their immediate supervisor or TIGTA's Office of Chief Counsel. The TIGTA Office of Chief Counsel can be reached via e-mail at *TIGTA Counsel Office or via telephone at (202) 622-4068.

40.7 Office of Preference Program.
The Office of Preference Program (OPP) is intended to proactively identify those OI employees who wish to be considered for a lateral reassignment. The program provides employees with the opportunity to make their personal needs and wishes known to the agency. Although OI management will consider employees' needs along with TIGTA's mission, mobility remains a condition of employment for all SAs. Relocation expenses are not authorized and administrative leave will not be granted for reassignments made under the OPP. Both supervisory and non-supervisory OI employees are eligible to participate in the program. See Chapter 600, Section 40.4.7.2.

The OPP does not replace TIGTA procedures for requesting hardship transfers, and does not take precedence over requests for hardship transfers. Participation in the OPP does not preclude SAs from applying for posted vacancies for which they are eligible. See Chapter 600, Section 70.6.9 for information regarding hardship transfers.

40.7.1 Basic Requirement for Participation. To be eligible for an OPP reassignment, the employee must meet the following requirements:

- Absent extenuating circumstances, the individual should be employed by TIGTA for at least three years; and
- The individual must have received at least a "successful" rating on the most recent performance appraisal record.

40.7.2 OPP Application Process. OPP requests may be submitted at any time. Interested employees must submit a written request to their second-level supervisor, through their immediate supervisor, expressing interest in participation in the OPP and identifying the desired assignment and post of duty (POD) for which he/she would like to be considered. The written request must be accompanied by a signed Moving Expense Waiver. See Exhibit (400)-40.5.

If either the SAC/Director of the "losing" division or the SAC/Director of the "gaining" division believes that honoring the OPP request would negatively impact either division, the OPP request is denied at the SAC/Director level. If the request is initiated by a SAC/Director, the reviewing DAIGI/AIGI will make the determination.

If both SACs/Directors agree that the request should be forwarded for further consideration, the OPP request will be submitted to the appropriate DAIGI/AIGI and the DIGI, as appropriate. The requestor will be notified that his/her request has been received. The respective OI executive will have a discussion with the requestor and the "gaining" and "losing" SAC/Director about his/her OPP request. The respective OI executive and the impacted SACs/Directors will discuss the request to determine the overall impact of the request on the Agency and whether or not the OPP request will be approved or denied.

If the OPP request is approved by the appropriate executive, the SAC/Director will notify the employee that the request was approved. If the OPP request is denied, the SAC/Director will notify the employee that the request was denied. If a SAC/Director initiated the OPP request, the appropriate executive will notify the employee of the determination.

40.7.2.1 Limitation on Requests. Employees are limited to a total of three requests for reassignment/POD preference at any one time and must submit a separate request for each requested assignment/POD. OPP requests will be confirmed annually. If the employee no longer wishes to be considered for a reassignment or change in POD, his/her name will be removed from the OPP.

40.7.2.2 Withdrawal from the OPP. Employees may withdraw from the OPP at any time by submitting a written statement to their second-level supervisor through their immediate supervisor. The second-level supervisor will forward the notification to withdraw from the OPP to the appropriate DAIGI/AIGI, or DIGI, as appropriate.

If the employee's personal needs or desires change and they wish to withdraw their OPP request, the employee should immediately notify their second-level supervisor, through their immediate manager. The second-level supervisor will immediately notify the appropriate DAIGI/AIGI, or DIGI, as appropriate, of this request.

The employee may reapply at any time in the future.

40.7.2.3 Declining OPP Placement. If an employee decides to decline a placement opportunity made through the OPP, the employee must submit a written statement to his/her second-level supervisor, through the immediate supervisor, stating his/her name, the date of declination, and the assignment/POD declined. The second-level supervisor will forward the statement to the appropriate DAIGI/AIGI. The employee will be removed from the OPP roster for that assignment/POD.

The employee may reapply at any time in the future.

40.7.2.4 Reassignment. When an employee is selected for a lateral reassignment through the OPP, the SAC/Director of the "losing" division will negotiate a reporting date for the requesting agent with the "gaining" division. If the request is initiated by a SAC/Director, the reviewing DAIGI/AIGI will make the determination.

40.7.3 Selection Criteria. OI management will avoid placements that could negatively affect a division. OI management will consider several factors, including, but not limited to, the following when evaluating OPP requests:

- Vacancy(ies) at the requested post of duty;
- Overall impact to the agency and division;
- Other individuals from the same group who have submitted OPP requests;
- The impact the transfer will have on the skill level of the group/division;
- The impact the transfer will have on any collateral duties; and
- The impact the transfer will have on space needs.

If more than one OPP request is submitted for a position, seniority may be a factor in the selection of one candidate over another.

Submission of the OPP request does not guarantee that the employee will be reassigned. OI management reserves the right to deny a request for a lateral reassignment through the OPP. OI management may fill vacancies by other means available to them and is not required to select from the OPP.

40.7.3.1 Eligibility Determination. When an opening is anticipated in an assignment/POD, the SAC/Director will contact the respective DAIGI/AIGI for a list of employees on the OPP roster for that assignment/POD. The SAC/Director will verify the current eligibility of each interested employee by requesting a copy of his/her most recent performance appraisal.

40.7.3.2 Initiating Placement. Once the placement has been approved, the SAC/Director of the "gaining" division can then contact the SAC/Director of the "losing" division to determine a mutually agreeable reporting date. Placements, effective dates, and reporting dates may not be finalized without the involvement of the Bureau of the Fiscal Service's (BFS) Administrative Resource Center.

To initiate a placement under this program, the "losing" SAC will ensure that the Standard Form 52 (SF 52), *Request for Personnel Action*, is submitted to BFS via HR Connect. The following comment should appear in the Remarks section: "Placement of [Title of Employee] [Full Name] under the Office of Preference Program."

40.8 Collateral Duties.
Collateral duties are official duties and responsibilities assigned to an SA in addition to the primary duties and responsibilities of the SA position.

Collateral duties for individual SAs should be monitored and balanced with their investigative inventory. Collateral duties assigned to SAs are as follows:

- Evidence Custodian – See Section 190.5.1 of this chapter for evidence custodian duties;
- HIP Coordinator– See Section 90.4 of this chapter for HIP Coordinator duties;
- Divisional Victim Witness Coordinator (DVWC) – See Section 230.3.2 of this chapter for DVWC duties;
- Technical Services Officer (TSO) – See Section 160.6.3 of this chapter for TSO duties;
- Defensive Tactics Coordinator (DTC) – See Section 130.3.1.5 of this chapter for DTC duties;
- Divisional Firearms, Agent Safety, and Training (FAST) Coordinator (DFC) – See Section 130.3.1.3 of this chapter for DFC duties;
- Firearms Instructor – see Section 130.3.1.4 of this chapter for Firearms Instructor duties;
- On-the-Job Training Instructor (OJI) – See Section 100.5.3.4 of this chapter for OJI duties; and
- Criminal Intelligence Coordinator (CIC) – See Section 410.13 of this chapter for CIC duties.
- TECS System Control Officer (SCO) – See Section 150.4 of this chapter for law enforcement databases.

DATE: October 1, 2017

CHAPTER 400 – INVESTIGTATIONS

(400)-50 Official Passports

50.1 Overview.
This section contains information regarding official passports and provides policies and procedures for Treasury Inspector General for Tax Administration's (TIGTA) Office of Investigations (OI) employees who perform official travel in the interest of the Federal Government, who require an official passport. It is also for managerial and administrative personnel who authorize, direct, and review travel arrangements that require an official passport issued by the U.S. Department of State's Special Issuance Agency (SIA).

50.1.1 Acronym Table.

50.2 Authorities.
TIGTA's OI follows the guidance outlined in C.F.R. Title 22 Chapter 1 regarding the authorities associated with official passport issuance.

50.3 Foreign Travel and Official Passports.
Employees traveling on official business to any foreign country, including Canada or Mexico, require an official passport. Official passports are issued by the U.S. Department of State's SIA. All official passports remain the property of the U.S. Department of State and are to be used for official business only.

The SIA office of the U.S. Department of State issues passports to citizens traveling abroad for the U.S. Government. The type of passports issued are: Diplomatic (black cover), Official (red/maroon cover), No-Fee Regular (blue cover), and Service (gray cover). The SIA will determine which type of passport is to be issued based on the travel purpose provided by the traveler. In general, TIGTA personnel will be issued an official passport (red/maroon cover).

An official passport is required when traveling to a foreign country for the purpose of official business. If an employee intends to combine personal travel in conjunction with their official travel, he/she must utilize their non-fee regular passport (blue cover), not their official passport (red/maroon cover). Official passports are not to be used for personal travel. Due to the nature of OI's investigative mission and investigations related to an international nexus, official passports may be issued to employees who have an official international trip, or in order to increase our investigative posture and response capability and mission readiness related to international cases. The U.S. Department of State will only issue one official passport to a Federal employee.

Travelers should submit their request for an official passport as soon as they anticipate travel for official business outside the U.S.

50.3.1 Intelligence Reform and Terrorism Prevention Act of 2004 and the Western Hemisphere Travel Initiative. The Western Hemisphere Travel Initiative requires all citizens of the U.S., Canada, Mexico, and Bermuda to have a passport or other accepted documents that establish the bearer's identity and nationality to enter or depart the U.S. from the Western Hemisphere.

50.4 Request for an Official Passport.
Travelers must prepare an authorization letter for orginal signature by the Deputy Inspector General for Investigations (DIGI), or an authorized designee. See Exhibit (400)-50.1

50.4.1 Supporting Documentation. If employees have not previously had *any* type of passport, a U.S. passport more than 15 years old, were under the age of 16 when they applied, or their last U.S. passport was lost, stolen or damaged, they must prepare a Form DS-11, U.S. Passport Application, available online at U.S. Department of State's Website. The following documents will be needed:

- Recent Standard Form (SF) 50
- Proof of U.S. Citizenship (*e.g.*, birth certificate or any documentary evidence shortly after birth but generally not more than five years after birth)
- Proof of identity, plus one copy of proof of identity on an 8 x 11 size white paper.
    - The copy must include the front and back of the document; and
- Two recent identical standard passport photos (2 x 2 color portrait), and the requirements are:

    - Taken in the last six (6) months;
    - Appropriate attire without hat or headgear that obscures the hairline (unless worn for religious reasons);
    - Uniforms must NOT be worn (military or military-like attire unacceptable);
    - Hearing device, wigs, facial jewelry, *etc.*, can be worn in the photo if they are consistently worn; and

- As of November 1, 2016, prescription and non-prescription glasses should not be worn in the photo. If glasses, can not be removed for medical reasons an accompanying medical certificate is required.

Note: A valid or expired U.S. Department of State Passport (Diplomatic, Official or Regular No-Fee) that is not damaged will meet both citizenship and identity requirements. The U.S. Department of State will return original documents to the applicant.

50.4.2 2-D Barcode for Online Passport Application. A fillable Form DS-11 may be located on the U.S. Department of State's Website. An application for U.S. Passport or Registration may be completed online prior to printing. The application contains a 2-D barcode. Once the applicant completes Form DS-11, a barcode will appear on the left side of the first page of the passport application. The barcode is encrypted with the information contained in the application. The 2-D barcode application will reduce the occurrence of incomplete applications and mistakes made during the processing of the form. The barcode application also shortens the processing period.

In order to complete the 2-D barcode application, applicants must go the U.S. Department of State's Website. The data entered in the online form will be verified. If there are errors, applicants will be prompted to make corrections. If there are no errors, the Form DS-11 will be generated in a PDF format and returned as a downloaded file. Applicants may save the file. The online form must be printed single-sided. The U.S. Department of State will not accept double-sided forms. All data fields and the barcode must be complete and clear. Applications with any distortions, fading, and smudges may be rejected. **Do not sign the form** until it is witnessed by a U.S. Department of State certified passport acceptance clerk or agent, who must administer an oath to the applicant. "Address Line 2" should be annotated with TIGTA's assigned agency code, TS/IGTA. Employees must have their form witnessed by a passport acceptace clerk or agent.

50.4.2.1 Name Changes. If your name changes (*e.g.*, marriage, divorce) within one year of the date your official passport was issued, submit a U.S. Department of State Form DS-5504, *Application for U.S. Passport: Name Change, Data Correction, and Limited Passport Book Replacement*, in accordance with the instructions provided within the form. If the name change occurs more than one year after your official passport was issued, submit a U.S. Department of State Form DS-82, *Application for Passport by Mail*, in accordance with the instructions provided within the form.

50.4.3 Employees Located in Headquarters. Employees applying for an official passport must have their form witnessed by a U.S. Department of State certified passport acceptace clerk or agent. The TIGTA OI Passport Coordinator is a passport acceptance clerk or agent, can certify the supporting documentation, and can witness the employee's signature. The TIGTA OI's Passport Coordinator will hand-carry the package to the SIA.

50.4.4 Employees Located outside of Headquarters. Employees applying for an official passport who are physically located outside of the Washington, DC, commuting area must find a local U.S. passport servicing office near them to accept and process the passport request. This passport servicing office is usually located inside a U.S. Post Office. Employees must contact the TIGTA OI's Passport Coordinator to obtain the original authorization letter. The authorization letter will allow the local passport acceptance clerk or agent to accept and process the official passport request from TIGTA.

Employees must present the agency's original authorization letter (plus one copy of the letter for the local passport clerk or agent); the completed application Form DS-11; and the supporting documentation to their local U.S. Passport Office or passport servicing agency. At that location, the authorized passport acceptance clerk or agent will certify the supporting documentation and sign the application.

50.4.5 Authorized Pick Up. When the SIA has prepared the official passport, they will notify TIGTA OI's Passport Coordinator that the passport is ready to be picked up. Only TIGTA-authorized individuals (such as TIGTA OI's Passport Coordinator) may pick up official passports. Once authorized personnel have picked up the passport from the SIA, TIGTA OI's Passport Coordinator will express-mail (outside TIGTA Headquarters) or hand-carry (at TIGTA Headquarters only) the passport to the employee. Employees must sign their passport before it may be used.

Employees should request that the local passport acceptance clerk or agent mail the package to the SIA using a traceable confirmation method via overnight express delivery. The local passport acceptance clerk or agent may charge the employee an execution fee. If so, the employee may use their Government issued travel card to pay for this one-time fee, including applicable postage fees, or the employee may file a local travel voucher for reimbursement and submit when appropriate. See (600)-40.5.35.1 for additional information.

50.5 Electronic Passports.
On December 30, 2005, the U.S. Department of State began phasing-in the issuance of the new electronic passport (e-passport) to better facilitate international travel for U.S. citizens and enhance border security. The electronic format for official passports is currently being issued. Renewed passports will be upgraded with the e-passport technology.

The new passport combines face recognition and contactless chip technology. The chip is embedded in the cover of the passport and holds the same information that is printed in the passport: name, date of birth, gender, birthplace, passport issuance date and expiration date, passport number, and the photo image of the bearer.

To address privacy concerns, the U.S. Department of State has incorporated an anti-skimming device in the e-passport's front cover. The e-passports will also include Basic Access Control (BAC) technology to prevent skimming and eavesdropping. The combination of the anti-skimming device and the BAC technology is intended to mitigate unauthorized reading of e-passports.

50.6 Visa Requirements.
Some countries require the traveler to obtain a visa in addition to having a passport. Employees must determine the need for a visa for an impending trip prior to applying for an official passport, and prior to traveling in the future with a valid official passport. The need for a visa must be noted in their memorandum to the DIGI, or authorized designee. Employees can determine the need for a visa from the U.S. Department of State's Website and by consulting their contact(s) in the country(ies) they plan to visit. It is the responsibility of the Trip Coordinator (usually at Treasury's Office of Technical Assistance [OTA]) to obtain the visa. The Trip Coordinator will need the signed official passport to obtain a visa. Employees should plan on five workdays to obtain a visa. TIGTA OI's Passport Coordinator is only involved in the process of obtaining a visa when the trip is sponsored by TIGTA; in other cases, employees should work directly with the Trip Coordinator.

50.6.1 Additional Visa Pages. Travelers are responsible for ensuring sufficient visa pages are available in their Government passports before their trip. Travelers should complete and forward Form DS-4085, Application for Additional Visa Pages or Miscellaneous Passport Services, (available on the U.S. Department of State's Website) along with their official passport (if not already in the possession of TIGTA OI's Passport Coordinator) for processing to the SIA. Travelers should allow at least one week to complete processing.

50.7 Country Clearance.
While this is not an Official passport requirement, employees should be aware that traveling to a foreign country with an official passport may require a country clearance. This is an electronic confirmation by the U.S. Department of State that the employee can travel to that country for official business. It is the responsibility of the agency sponsoring the trip to arrange for country clearance when needed. Employees must provide their travel itinerary (flight/hotels), personal/business contact information, and country contact information.

50.8 Renewal of Official Passports.
Employees should be aware of when their official passport will expire. Employees who have an official passport that will soon expire must timely request a new official passport. Official passports are issued with a five year expiration date.

Employees who have an official passport that will expire (but is still valid) before completing future planned foreign travel arrangements, should complete Form DS-82, Application for Passport Renewal by Mail, available on the U.S. Department of State's

Website. The completed DS-82, along with the current official passport and two new passport photos should be forwarded to TIGTA OI's Passport Coordinator at least 30 days prior to the expiration date of the current official passport. These documents should be attached to the required memorandum to the DIGI, or his/her authorized designee. TIGTA OI's Passport Coordinator will prepare the authorization letter and forward the package to the SIA.

50.9 Official Passports obtained through Other Agencies.
Employees who already have an official passport obtained from another Federal agency should send the passport along with a memorandum explaining they are separating from the agency to the SIA. To retrieve the passport for official travel business with the new Federal agency, the employee can submit Form DS-4085 along with a memorandum requesting to release the passport from the SIA to TIGTA OI's Passport Coordinator. TIGTA OI's Passport Coordinator will prepare and provide an authorization letter to the SIA. The reissued official passport will be released back to TIGTA OI's Passport Coordinator who will return it to the employee. Employees do not need specific planned foreign trips in order to have their official passport reissued through TIGTA.

50.10 Immunization Requirements.
An "International Certificate of Vaccination" is required for U.S. residents visiting foreign countries. Canada and a few other countries do not require this certificate. Prior to traveling internationally, travelers should obtain guidance about specific immunization requirements and obtain the certificate from the nearest Office of the United States Public Health Service. Immunization expenses for the purpose of official business may be charged to the cardholder's individually-billed account (IBA). However, pre-approval to incur immunization charges on the IBA must be obtained from the Office of Mission Support in order to temporarily unblock medical merchant codes on the cardholder's IBA.

Travelers should use U.S. Government facilities, including the United States Public Health Service, for required immunizations when available and practical. Travelers using the services of a private physician may claim reimbursement on their travel voucher. Employees located in Washington, DC, may use the U.S. Department of State's facilities once they have received their travel authorization.

50.11 Official Passport Custody and Location.
The official passport remains the property of the Federal Government. Agencies must maintain control over and the use of both official and diplomatic passports. Upon issuance of an official passport, the employee's supervisor will prepare a Form OI 1930, Custody Receipt for Government Property, for signature by the employee. Once the employee signs the Form OI 1930 the supervisor may issue the passport to the employee. The supervisor will maintain a copy of both the passport and Form OI 1930 in the employee's drop file.

OI personnel will maintain possession of their official passport and be responsible for the custody and security of their passport. The official passport will be inspected annually by the supervisor along with other accountable property. This physical inspection will be documented on the Accountable Properties Certification. A lost or stolen official passport should be reported to the TIGTA Personnel Security Officer through the employee's management chain, so that it can be cancelled by the U.S. Department of State.

50.12 Security Clearance.

Travel to foreign areas may require a security clearance if official duties are being performed at an Embassy or Consulate. The valid levels of security clearances are Confidential, Secret, or Top Secret. Questions may be directed to TIGTA OI's Passport Coordinator who will coordinate the needed actions, including any necessary coordination with TIGTA's Personnel Security Officer. For related questions regarding your security clearance you may e-mail *TIGTA Personnel Security Office.

DATE: April 1, 2019

CHAPTER 400 – INVESTIGATIONS

(400)-60 General Legal Matters

60.1 Overview.
This Section contains administrative instructions and general information for TIGTA-Office of Investigations (OI) personnel, including:

- Giglio Policy
- Right to Financial Privacy Act of 1978
- Peace Officer Status and Scope of Employment

60.1.1 Acronyms Table.

60.2 Giglio Policy.
For Giglio policy information, see TIGTA Operations Manual, Chapter (700)-90.8, *Giglio/Henthorn Policy*.

60.3 Right to Financial Privacy Act of 1978.
The Right to Financial Privacy Act of 1978 (RFPA) generally prohibits government access to, and a financial institution's disclosure of, the financial records of certain customers. The RFPA does not apply to bank records of corporations, associations, or larger partnerships. There is an exception to the general rule against access/disclosure for a legitimate law enforcement inquiry complying with one of the prescribed methods of access.

The RFPA provides civil penalties for violations by financial institutions and Federal agencies. The RFPA also provides for disciplinary proceedings by the Office of Personnel Management (OPM) to determine if a Federal officer willfully or intentionally violated the RFPA.

60.3.1 Definitions Used In the RFPA. The following definitions apply to the RFPA:

- **Person –** is an individual or partnership of five or fewer individuals. The RFPA does not apply to bank records of corporations, trusts, associations, or larger partnerships. It also does not apply to deceased account holders.
- **Customer –** is any person or authorized representative of that person who is using or has used any service of a financial institution, or for whom a financial institution is acting or has acted as a fiduciary to an account maintained in the person's name.
- **Financial institution –** is any office of a bank, savings bank, credit card issuer, industrial loan company, trust company, savings and loan, homestead association including cooperative banks, credit union, or consumer finance

institution located in any State or territory of the United States, Puerto Rico, Guam, American Samoa, or the Virgin Islands.

- **Financial record –** is an original of, copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution. The account must be in the customer's true name. Accordingly, the RFPA does not apply to forged or counterfeit financial instruments or records concerning an account maintained under a fictitious name.
- **Law enforcement inquiry –** is an official lawful investigation of a violation of any criminal or civil statute, regulation, rule or order.

60.3.2 Basic Requirements of the RFPA. The RFPA imposes certain basic requirements regarding:

- Restrictions on government access;
- Government certification of compliance with the RFPA;
- Notice to customer;
- Challenge;
- Appeals;
- Notification of legal proceedings;
- Delay of notice; and
- Use of information.

60.3.3 Restrictions on Government Access. The RFPA prohibits any government authority, Federal department or agency from accessing or obtaining from a financial institution copies of, or accessing or obtaining the information contained in, the financial records of any customer unless the financial records are reasonably described and disclosure is authorized by either:

- Customer consent;
- Administrative subpoena or summons; (see Section 220 of this Chapter for additional information regarding administrative subpoenas);
- Search warrant;
- Judicial subpoena; or
- A formal written request.

OI special agents (SAs) are not authorized to use a formal written request to obtain financial records under 31 CFR § 14.3, because TIGTA has administrative subpoena authority pursuant to the Inspector General (IG) Act.

60.3.4 Government Certification of Compliance with RFPA. A financial institution will not release financial records of a customer until the government authority seeking such records certifies in writing that it has complied with all applicable provisions of the

RFPA. Such certification relieves the financial institution of any liability to the customer in connection with the disclosure of the financial records. See TIGTA Form OI S-012, *Certificate Of Compliance With The Right To Financial Privacy Act,* for sample certification format.

60.3.5 Notice to Customer. The RFPA requires that a customer of a financial institution be given prior notice of the attempt of a government authority to gain access to records or record information held by the financial institution concerning such customer. See TIGTA Form OI S-005, *Customer Notice Form,* for the notice required to be given with a judicial subpoena or administrative subpoena. The notice to the customer is accompanied by a motion paper and sworn statement, which the customer may use to try to quash the subpoena. See TIGTA Form OI S-008, C*ustomer's Motion To Challenge Government Access To Financial Records,* and TIGTA Form OI S-009, *Customer's Sworn Statement For Filing A Challenge Form,* for samples of each. Customers do not have to use these forms.

60.3.6 Motions to Quash and Applications to Enjoin. The RFPA provides that the customer of a financial institution may challenge the government's access to his or her records if, within 10 days of service or 14 days of mailing a subpoena or formal written request, the customer files in the appropriate Federal court a motion to quash the administrative subpoena or judicial subpoena or an application to enjoin a government authority from obtaining access pursuant to a formal written request. If the customer files a motion to quash and, in the opinion of the court, complies with the RFPA's procedural requirements, the court will order the government to file a sworn response.

The government authority may file its response *in camera,* if the response includes the reasons which make *in camera* review appropriate. This should only be done if it is necessary to protect the investigation, the safety of witnesses, or to avoid improper discovery practices.

The government response should set forth the reason why the investigation is proper and why the records are relevant. The government bears the burden of proving substantial compliance with the RFPA's requirements for access to the customer's financial records. If the court finds that the financial records sought pertain to an investigation within the law enforcement agency's jurisdiction and that the records sought are relevant to that inquiry, it will deny the motion or application, and in the case of an administrative summons or court order other than a search warrant, order such process enforced. The RFPA contemplates that the motion to quash or application will be decided within seven calendar days of the filing of the government's response.

60.3.7 Appeals. A court ruling denying a customer's motion to quash is not a final order and an interlocutory appeal may not be taken by the customer. If no legal proceeding is to be commenced against the customer, an appeal may be made within 30 days of a notification to that effect.

The U.S. Attorney's Office (USAO) can appeal an adverse final judgment. The customer must be notified within 30 days of the USAO's decision to appeal an adverse ruling. An appeal may be taken within 30 days of such notification. In the event that no determination regarding a legal proceeding is made within 180 days, a certification may be required by the court until the investigation is concluded.

60.3.8 Delayed Notice. The government authority may apply to an appropriate court to delay the required notice to the customer for as much as 90 days and to issue an order prohibiting the financial institution from disclosing that records have been obtained or that a request for records has been made. Such delay may be granted if the court finds that notice to the customer will result in endangering the physical safety of any person, cause flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, or seriously jeopardizing an investigation or official proceeding. Additional extensions of 90 days may be granted by the court upon application. Upon expiration of the delay of notification, the customer shall be served with a copy of the process or request together with TIGTA Form OI S-013, *Post-Notice Following Court-Ordered Delay.*

60.3.9 Transfer of Information. Financial records that OI SAs originally obtain pursuant to the RFPA shall not be transferred to any other agency or department, including the Department of Justice (DOJ), unless TIGTA certifies in writing that there is reason to believe that the records are relevant to a legitimate law enforcement inquiry within the jurisdiction of the receiving agency or department. After consulting with TIGTA Counsel, the appropriate Assistant Inspector General for Investigations (AIGI) shall sign the appropriate certification and forward a copy to TIGTA Counsel. In addition, within 14 days of the transfer, the ASAC shall send a copy of the certification to the customer notifying him/her of the nature of the law enforcement inquiry and his/her rights pursuant to the RFPA. Court orders may be used to delay this notice. See TIGTA Form OI S-014, *Certification For Transferring Records Obtained Pursuant To The Right To Financial Privacy Act Of 1978,* and TIGTA Form OI S-015, *Notice Of Transfer Of Financial Records.*

60.3.10 Exceptions and Special Procedures. Exceptions or special procedures are provided for:

- Disclosure to a government authority authorized to conduct foreign counter, or foreign positive, intelligence activities for purposes of conducting such activities;
- Disclosure to the U.S. Secret Service for the purpose of conducting its protective functions;
- Disclosure of financial records or information in accordance with the Internal Revenue Code;

- Disclosure to, or examination by, a supervisory agency pursuant to the exercise of supervisory, regulatory, or monetary functions with respect to financial institutions, holding companies, subsidiaries, institution-affiliated parties or other person participating in the conduct of the affairs thereof;
- Disclosure pursuant to a Federal statute or rule promulgated thereunder;
- Voluntary disclosure of information to governmental authorities pertaining to possible violations of law, limited to the name or identifying information concerning the individual, corporation or account involved in, and the nature of, any suspected illegal activity;
- Disclosure pursuant to a legitimate law enforcement inquiry respecting name, address, account type and number of particular customer or ascertainable group of customers associated with a financial transaction or class of financial transactions or with a foreign account in the United States under § 5(b) of the Trading with the Enemy Act; the International Emergency Economic Powers Act; or § 5 of the United Nations Participation Act;
- Disclosure of financial records not identified with or identifiable as being derived from a particular customer;
- Disclosure pursuant to the Federal Rules of Criminal and Civil Procedure or comparable rules of other courts in connection with litigation to which the government authority and the customer are parties;
- Disclosure pursuant to an administrative subpoena issued by an administrative judge and to which the government authority and the customer are parties;
- Disclosure pursuant to a lawful investigation, proceeding, examination, or inspection directed at a financial institution, or legal entity, whether or not also directed at a customer or at a legal entity which is not a customer; or in connection with the authority's consideration or administration of assistance to the customer in the form of a government loan, loan guaranty, or loan insurance program. Financial records obtained pursuant to this subsection may be transferred to another agency or department only to facilitate a lawful investigation, proceeding, examination or inspection directed at a financial institution, whether or not also directed at a customer, or at a legal entity which is not a customer;
- Disclosure pursuant to a lawful proceeding, investigation, etc., directed at a financial institution or legal entity or consideration or administration respecting government loans, loans guarantees, etc.;
- Disclosure pursuant to the issuance of a subpoena or court order respecting grand jury proceedings;
- Disclosure pursuant to a proceeding, investigation, etc., instituted by the Government Accountability Office and directed at a government authority;
- Disclosure of any financial record or information to a government authority in conjunction with a Federal contractor-issued travel charge card issued for official government travel; and

- Disclosure of financial records from a financial institution to a government authority, if the government authority determines that delay in obtaining access to such records would create imminent danger of physical injury to any person; serious property damage; or flight to avoid prosecution. The existence of any of the above-referenced situations will be addressed as an emergency situation. See Section 60.3.15 and Section 220 of this Chapter.

60.3.11 Methods of Accessing Financial Records. Access financial records by any of the following methods:

- Administrative subpoena, as detailed in Section 220 of this Chapter;
- Customer authorization;
- Search warrant; or
- Judicial subpoena.

60.3.12 Customer Authorization. The customer may authorize disclosure if he or she furnishes to the financial institution and to the government authority seeking to obtain such disclosure a signed and dated statement which:

- Authorizes such disclosure for a period not in excess of three months;
- States that the customer may revoke such authorization at any time before the financial records are disclosed;
- Identifies the financial records which are authorized to be disclosed;
- Specifies the purposes for which, and the government authority to which, such records may be disclosed; and
- States the customer's rights. See Form OI S-004, *Customer Authorization To Release Financial Record,* and Form OI S-006, *Statement Of Customer Rights Under The Right To Financial Privacy Act Of 1978.*

60.3.13 Search Warrant. A government authority may obtain financial records by using a search warrant only if it obtains the search warrant pursuant to the Federal Rules of Criminal Procedure. Unless a U.S. District Court grants a delay, no later than 90 days after the issuance of a search warrant, the government authority must mail a copy of the search warrant to the customer's last known address along with a notice similar to Exhibit (400)-60.2.

Upon expiration of the period of delay of notification of the customer, mail to the customer a copy of the search warrant and a notice similar to Exhibit (400)-60.3.

60.3.14 Judicial Subpoena. A judicial subpoena is an order of a court that requires a person to be present at a certain time and place or suffer a penalty. A subpoena *duces tecum* is an order of a court requiring the production of documents. A copy of the subpoena is served on the customer or mailed to the last known address on or before

the date the subpoena is served on the financial institution, together with the notice to the customer, a motion paper, and sworn statement. See TIGTA Form OI S-007, *Instructions For Completing And Filing The Customer's Challenge Motion And Sworn Statement*, OI S-008 and OI S-009.

60.3.15 Emergency Access. When there is reason to believe that delay in obtaining financial records from a financial institution would create imminent danger of physical injury to any person, serious property damage, or flight to avoid prosecution, submit to the financial institution the certification of compliance with the RFPA. See Form OI S-012. In addition:

- Within five days of access, a sworn statement setting forth the grounds for emergency access by a TIGTA official must be filed with the appropriate court; and
- As soon as possible after the records have been obtained, unless a delay order is instituted, mail or serve a copy of the request together with notification of emergency access to the customer. See Exhibit (400)-60.1 for sample format.

60.3.16 Cost Reimbursement. Title 12, United State Code § 3415 caused the Federal Reserve Board to set the rates and conditions for reimbursement of reasonably necessary costs directly incurred by financial institutions in providing customer financial records to Federal agencies. Upon receipt of an invoice for records provided by any entity as the result of a subpoena, the field office will forward the invoice via electronic mail to the *TIGTA Inv Operations inbox. See Section 220.7.2 of this Chapter for details on cost reimbursement for compliance with subpoena requests.

60.4 Peace Officer Status and Scope of Employment.
Title 28, United States Code § 1442 provides that a Federal law enforcement officer (LEO) shall be construed to be acting within the scope of his or her employment if the LEO takes reasonable action, including the use of force, to:

- Protect an individual in the presence of the officer from a crime of violence;
- Provide immediate assistance to an individual who has suffered or who is threatened with bodily harm; or
- Prevent the escape of any individual who the officer reasonably believes to have committed in the presence of the officer a crime of violence.

OI SAs have authority to act on Federal offenses, but the ability to support local partners and stakeholders in a local law enforcement capacity depends on whether SAs have peace officer status in a State. Each State defines peace officer status differently, but the status generally refers to the authority to perform State and local law enforcement functions in a specific jurisdiction. SAs should understand the peace officer status in their respective jurisdictions.

60.4.1 Law As It Applies to OI Special Agents. An SA who acts as a peace officer under State law is not protected by the Federal Tort Claims Act, and may be personally liable for negligent acts.

While a State may confer peace officer authority upon Federal LEOs, the State cannot broaden the Federal jurisdictional limits of OI SAs established by Congress. A State may not impose a duty upon OI SAs to enforce its State criminal laws.

60.4.2 Liability – When Acting as a Peace Officer. Unless an action is covered by 28 U.S.C. §1442 or other applicable Federal law:

- OI SAs may face civil or criminal prosecution in State court;
- OI SAs may be held individually liable for damages absent State legislation or judicial decision affording indemnification under State law to peace officers;
- The U.S. Government may not be held liable for such actions nor may the Federal government indemnify Federal LEOs for damages assessed against them. TIGTA does not have the authority to pay any adverse judgment rendered against an employee acting outside the scope of his or her employment
- An SA may not have the benefit of the qualified immunity afforded Federal employees acting within the scope of their employment and may not have the benefit of the defense of qualified immunity if their actions became the subject of litigation under 42 U.S.C. § 1983; and
- Benefits may not be paid under the Federal Employees Compensation Act (FECA) to OI SAs who were injured as a result of actions taken in the capacity of peace officers. The Department of Labor has discretion as to who will be eligible for benefits under the FECA.

DATE: July 1, 2018

CHAPTER 400 – INVESTIGATIONS

(400)-70 Disclosure Authority

70.1 Overview.
This section includes instructions and procedures for TIGTA-Office of Investigations (OI) employees concerning the following:

- Authorized Access and Disclosure by TIGTA Special Agents
- Disclosure Authority under 26 U.S.C. § 6103
- Disclosure Authority under the Privacy Act
- Prosecutive Referrals
- Investigative Referrals to a Law Enforcement Agency
- Joint Investigations
- Accounting for Disclosures

70.1.1 Acronyms Table.

70.2 Authorized Access and Disclosure by TIGTA Special Agents (SAs).
Chapter 700 of the TIGTA Operations Manual Sections 50 and 70 discuss 26 U.S.C. § 6103 and the Privacy Act, 5 U.S.C. § 552a. These manual sections provide a discussion of the authority to access and disclose information protected by § 6103 and/or the Privacy Act.

For the purposes of § 6103 and/or the Privacy Act, investigations performed by TIGTA can be divided into the following three categories:

- Title 26 Tax Administrative Investigations;
- Non-Title 26 Tax Administration Investigations; and
- Other Investigations (Non-Tax Administration).

Each category of investigation identified above carries with it unique rules related to an SA's authority to access or disclose information protected by § 6103 and/or the Privacy Act. SAs must understand these rules to avoid an unauthorized access (UNAX) or disclosure of protected information in violation of the law.

70.2.1 Category I – Title 26 Tax Administration Investigations. In this category, the allegation being investigated by TIGTA is a violation of a criminal or civil provision of the Internal Revenue Code, Title 26 of the United States Code. Examples of this category include allegations of violation of 26 U.S.C. § 7212, 26 U.S.C. § 7213, 26 U.S.C. § 7213A, 26 U.S.C. § 7214, and violations of § 1203(b)(8) and (b)(9) of the IRS Restructuring and Reform Act of 1998 (RRA 98), and § 1203(b)(6) of the Internal Revenue Service Restructuring and Reform Act of 1998 (RRA 98) relating to violations

of the Internal Revenue Code. All Title 26 investigations are tax administration investigations.

70.2.1.1 Access to § 6103 Information in Category I Investigations. SAs conducting investigations of Title 26 tax administration allegations are authorized to access tax returns, Integrated Data Retrieval System (IDRS), or any other return information only if they have a need to know the information for use in the Title 26 investigation.

70.2.1.2 Disclosure Authority in Category I Investigations. Information created or obtained during a Title 26 investigation is the return information of the subject of the investigation. Further, many Title 26 investigations will also contain third party return information collected pursuant to the investigation, *e.g.*, UNAX or unauthorized disclosures. Thus, acknowledging the existence of an investigation into an alleged violation of the Internal Revenue Code is a disclosure that must be authorized by § 6103. The information collected during the investigation of an individual is also subject to the provisions of the Privacy Act.

70.2.2 Category II – Non-Title 26 Tax Administration Investigations. In this category, the allegation being investigated is not a violation of Title 26, but the alleged violation pertains to tax administration. Tax administration is defined in 26 U.S.C. § 6103 as the "administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws or related statutes." Not every investigation involving an Internal Revenue Service (IRS) employee (IRSE) is a tax administration investigation. Examples of tax administration investigations include bribery of an IRSE (18 U.S.C. § 201), embezzlement of taxpayer remittances (18 U.S.C. § 641), and violations of RRA 98, other than those sections referenced above.

70.2.2.1 Access to § 6103 Information in Category II Investigations. SAs conducting a tax administration investigation are authorized to access tax returns, IDRS, or any other return information only if they have a need to know the information for use in the tax administration investigation.

70.2.2.2 Disclosure Authority in Category II Investigations. The confidentiality provisions of § 6103 apply to all tax returns, IDRS, and other return information obtained during the tax administration investigation. The information gathered during the tax administration investigation is also subject to disclosure provisions of the Privacy Act.

70.2.3 Category III – Other Investigations (Non-Tax Administration). In this category, the allegation under investigation is not a violation of Title 26 and does not involve tax administration. Examples of this category include workers' compensation fraud, telemarketing fraud, mail fraud, bank fraud, wire fraud, false claims, etc.

70.2.3.1 Access to § 6103 Information in Category III Investigations. SAs conducting investigations that fall within this category are not authorized to directly access tax returns, IDRS, or any other return information from the IRS. If there is a need for § 6103 protected information in this type of investigation, SAs may only obtain tax returns, information from IDRS, or other return information by utilizing the provisions of § 6103(i), including obtaining an ex parte order.

70.2.3.2 Disclosure Authority for Category III Investigations. Generally, the confidentiality provisions of § 6103 will not apply to this category of investigations because SAs are not authorized to access § 6103-protected information during the investigation. In these circumstances, § 6103 only applies to tax returns and return information that may have been obtained through an ex parte order or other provision under § 6103(i). Information gathered in the investigation is, however, subject to the disclosure provisions of the Privacy Act.

If ...	Access...	Disclosure...
Category I – Title 26 Tax Administration Investigation	May access tax returns, IDRS, or return information if need to know	§ 6103 non-disclosure rules in effect for returns and return information including IDRS. Information collected is the subject's protected return information; may not disclose even the existence of the investigation. Privacy Act applies for individuals.
Category II – Non-Title 26 Tax Administration Investigation	May access tax returns, IDRS, or return information if need to know	§ 6103 non-disclosure rules in effect for the returns and return information including IDRS only; material must be kept confidential. Privacy Act applies for individuals.
Category III – Other Investigations (Non-Tax Administration)	May NOT access tax returns or return information including IDRS	§ 6103 non-disclosure rules do not generally apply; Privacy Act rules applies for individuals.

70.3 Disclosure Authority under 26 U.S.C. § 6103.
When information gathered by TIGTA is protected by the provisions of § 6103, TIGTA SAs are authorized to make the following disclosures:

- An SA may provide returns and return information to another Treasury employee who has a need to know the information for tax administration purposes [§ 6103(h)(1)];

- An SA may provide returns and return information to the Department of Justice (DOJ) for use in a tax administration proceeding [§§ 6103(h)(2) and (h)(3)];
- An SA may disclose a taxpayer's returns and return information to persons designated by the taxpayer by written consent [§ 6103(c)] (See (700)-50.5.2.1);
- An SA may make an investigative disclosure of return information (not tax returns) during a tax administration investigation when necessary to obtain information not otherwise reasonably available [§ 6103(k)(6)] (See text 70.3.1 of this Section);
- An SA may provide return information (not tax returns) to appropriate Federal or State officials in cases of imminent danger of death or physical injury, including threats against the President [§ 6103(i)(3)(B)(i)]; and
- An SA may disclose a taxpayer's returns and return information to persons as necessary in connection with the processing, storage, transmission, and reproduction of such returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and the providing of other services, for purposes of tax administration [§ 6103(n)].

70.3.1 Investigative Disclosure. SAs are authorized by § 6103(k)(6) (investigative disclosure) to disclose return information to the extent that such disclosure is necessary in obtaining information which is not otherwise reasonably available. This includes disclosures of return information to witnesses, as necessary. In addition, an investigative disclosure of return information may be made when necessary to persons possessing special expertise in areas such as handwriting analysis, photographic development, sound recording enhancement, voice identification, and polygraph. Section 6103(k)(6) permits the disclosure of return information in the investigation process, **but does not authorize the disclosure of returns themselves**.

When an investigative disclosure otherwise authorized under § 6103(k)(6) involves either the disclosure of voluminous return information or a long-term arrangement between TIGTA and the recipient of the disclosed return information, SAs should utilize a contractual agreement as authorized under § 6103(n). Preparation of an (n) contract should be coordinated with Operations Division, as needed.

70.3.2 Investigative Discussions. Official matters should not be discussed in public. Further, when a discussion of findings, theories, and plans relating to an investigation is necessary in order to achieve a better understanding of the investigation, the discussion should be limited to the TIGTA personnel directly concerned. This does not preclude discussions among SAs concerning investigative techniques, sources of information, etc.

70.4 Disclosure Authority under the Privacy Act.
When information gathered by TIGTA is protected by the provisions of the Privacy Act, TIGTA SAs are authorized to make the following disclosures:

- An SA may make disclosures to U.S. Attorney's Offices (USAO's) for prosecution with Assistant Special Agent in Charge (ASAC) concurrence. See Section 250.14 of this Chapter;
- An SA may provide information to another Treasury employee who has a need to know the information in the performance of their duties; and
- An SA may make disclosures, to include documents, to non-Treasury law enforcement officers (LEOs) during joint investigations for investigative purposes, if the LEO has a need for the information in order to pursue the investigation under his/her jurisdiction.

70.5 Prosecutive Referrals.
The procedures for referrals of information for prosecutive consideration depend on both the type of investigation and the intended recipient of the information.

70.5.1 Referrals to Federal Prosecutors. Under the provisions of both 26 U.S.C. § 6103 and the Privacy Act, SAs may, with the concurrence of the ASAC or higher-level manager, make appropriate referrals of cases to the USAO. Always document your discussions with the USAO on Form OI 6501, *Chronological Case Worksheet*. Information regarding both informal and formal referral procedures is contained in Section 250.14 of this Chapter.

70.5.2 Referrals to State/Local Prosecutors. All referral of written documents to the State/local prosecutor must be cleared through the Office of Chief Counsel (OCC). See Chapter 700, Chief Counsel, Section 70.5 for the procedure to request TIGTA OCC to review and clear an investigation for prosecutive referral to State/local prosecutors. TIGTA OCC will prepare the necessary record of disclosure form for these disclosures.

Prior to a formal (written) referral of assault cases, as well as Category II and III investigations, the SA must have an informal (oral) discussion with the State/local prosecutor in order to determine if the State/local prosecutor is interested in prosecuting a case with circumstances similar to those of the present investigation, but in hypothetical terms only. SA authorization to have **informal** (oral), hypothetical, discussions with a State/local prosecutor is dependent on the category of investigation (Category I, II, or III).

70.5.2.1 Referral to State/Local Prosecutors for Category I Investigations. As discussed in Chapter 700, Chief Counsel, Section 50.2, in an investigation of a Title 26 violation, all information collected during the investigation, including the Report of Investigation (ROI), is the return information of the subject. Further, information collected during many Title 26 investigations will also include the return information of

third parties, such as the information improperly accessed or disclosed in UNAX and unauthorized disclosure cases. Therefore, without a consent form signed by any applicable taxpayers, the ROI generally cannot be referred to State/local officials for prosecution, and SAs cannot engage in oral discussions, even in hypothetical terms. with State/local prosecutors regarding prosecutive consideration.

Note: An exception to this rule may exist for assault cases in which an individual has assaulted an IRSE because of the employee's position with the IRS. If the USAO declines to prosecute such a case federally, the case may, under certain circumstances, be referred to State or local officials for prosecution. Consult with TIGTA OCC for guidance prior to discussing assault investigations with a State prosecutor.

70.5.2.2 Referral to State/Local Prosecutors for Category II Investigations. Prior to the formal referral of a non-Title 26 tax administration investigation, the SA should determine if the State/local prosecutor is interested in prosecuting the case. See Chapter 700, Chief Counsel, Section 70.5. This informal discussion is often referred to as a "hypothetical" discussion. An SA may not discuss tax returns and/or return information during this discussion with the State/local prosecutor unless the SA has obtained a *Consent for Release of Tax Return and/or Return Information by the Treasury Inspector General for Tax Administration* signed by all taxpayer(s) involved.

In addition, the SA may not provide any information that would identify the subject of the investigation during the informal discussion.

The SA will be required to make an accounting for these "informal" disclosures. See text 70.8 of this Section regarding the accounting procedures.

70.5.2.3 Referral to State/Local Prosecutors for Category III Investigations. In a non-tax administration investigation, the ROI will generally not contain any tax return and/or return information unless the information has been obtained via ex parte order or other provision in § 6103(i). Generally, information obtained through the provisions of § 6103(i) cannot be referred to the State/local prosecutors other than under the terms of the (i) order or with a consent signed by all taxpayers whose return information is being disclosed.

Prior to the formal referral, the SA should determine if the State/local prosecutor is interested in prosecuting the case. See Chapter 700, Chief Counsel, Section 70.5. The TIGTA SA can only discuss the substance of the investigation in hypothetical terms during this informal referral, and cannot disclose any information that would identify the subject.

70.6 Investigative Referrals to a Law Enforcement Agency.
In the course of an investigation, SAs may develop information regarding allegations within the investigative jurisdiction of another law enforcement agency, both Federal and/or State/local. Referral of documents to another law enforcement agency must be referred through TIGTA's CC. See Chapter 700, Chief Counsel, Section 70.5 regarding Privacy Act Referrals, and Chapter 700, Chief Counsel, Section 70.5.1.1 for procedures.

70.7 Joint Investigations.
Treasury Inspector General for Tax Administration SAs sometimes conduct investigations of subjects who have allegedly violated a criminal statute that is also within the investigative jurisdiction of another law enforcement agency. The authority to investigate a case jointly with another law enforcement agency is governed by the type of investigation.

70.7.1 Joint Investigations Involving Category I and II Investigations. When conducting a tax administration investigation (Category I and II), TIGTA cannot work these cases jointly unless an Assistant United States Attorney (AUSA) has approved the joint investigation. The SA must ask the AUSA "for approval under § 6103 to work the case jointly with" another law enforcement agency in compliance with 26 CFR § 301.6103(h)(2) and DOJ Tax Division Directive 86–59. Even with an AUSA's approval under the provisions of § 6103 to jointly investigate a case, any disclosure of tax returns and/or return information must be made to the AUSA, who then may disclose to the other law enforcement agency. The AUSA may designate another law enforcement officer to be his/her recipient of the tax returns and/or return information.

70.7.2 Joint Investigations Involving Category III Investigations. In Category III investigations, the TIGTA SA may work the case jointly with another law enforcement agency. During the joint investigation, the TIGTA SA may make disclosures of information; to include documents collected during the course of the TIGTA investigation, with the concurrence of his/her ASAC. In instances where the SA is unsure what may or may not be disclosed, TIGTA OCC should be consulted prior to making the disclosure.

70.7.2.1 Making the Disclosure. In instances when TIGTA SAs are investigating a non-tax administration violation (Category III investigations), disclosure of information is subject to the provisions of the Privacy Act. TIGTA SAs may discuss the investigation with another law enforcement officer when:

- The LEO's office has jurisdiction over the statute involved; and
- The LEO has a need for the information in order to pursue the investigation under his/her jurisdiction.

70.8 Accounting for Disclosures.
The accounting provisions of the Privacy Act require that TIGTA SAs maintain a record of disclosures to AUSA's, State or local prosecutors, and other LEO's. See Chapter 700, Chief Counsel, Section 70.6 and the Privacy Act, 5 U.S.C. § 552a(c).

The accounting and safeguarding provisions of Title 26 require that TIGTA SAs make an accounting of disclosures made under 26 U.S.C. § 6103(i), Disclosure to Federal officers or employees for administration of Federal laws not relating to tax administration. See 26 U.S.C. § 6103(p)(3)(A).

Disclosures are required to be documented on the Form OI 6501 in the following instances:

- Referral to AUSA;
- Imminent danger referral to Federal/State law enforcement agency;
- Pre-referral (informal) discussion with State/local prosecutor in Category II investigations in which the SA discloses tax return and/or return information of a taxpayer who has signed a consent form; and/or
- Disclosures made to another law enforcement agency during a joint investigation.

The Form OI 6501 entry will contain the following information related to whom the information was disclosed:

- Name;
- Title;
- Address; and
- A description of the information disclosed.

DATE: July 1, 2017

CHAPTER 400 - INVESTIGATIONS

(400)-80 Criminal Results Management System (CRIMES)

80.1 Overview.
The Treasury Inspector General for Tax Administration's (TIGTA)-Office of Investigations (OI) CRIMES enhances the efficiency of OI's workflow, provides new statistical and analytical tools, allows for better case management for OI staff, as well as enables more effective tracking and reporting on OI's vital statistics. On November 1, 2016, CRIMES replaced OI's former Performance and Results Information System (PARIS) which was in place since April 2001. CRIMES provides TIGTA-OI the ability to manage and account for complaints received, including congressional inquiries, investigations initiated, and leads developed from Local Investigative Initiatives (LII) and National Investigative Initiatives (NII). It consists of a main navigation bar with eight work areas. The primary work areas are: workplace, activities, time management, RAFS and Help.

This section of the TIGTA Operations Manual provides for general instruction on the data to be captured in CRIMES. It is not meant to address other substantive policy issues that are more appropriately addressed elsewhere in the TIGTA Operations Manual. Additional resources relating to CRIMES may be obtained by visiting the CRIMES Help Guide Library. This section includes the following information related to CRIMES:

- CRIMES Terminology
- Responsibilities
- Intake/Case Numbering and Information Retrieval System
- Workplace Area
- Activities
- Time Management
- Request Assistance Forms (RAFS)
- Help

80.1.1 Acronyms Table.

80.2 CRIMES Terminology.
Helpful CRIMES terminology is outlined below:

- Forms – when the +New button is selected in any work area it will open a new form that will display required input data for a single record (intake, case, initiative, time summary, etc.).
- Navigation Bar – blue area at the top of the screen which provides the path taken to the screen the user is currently on and allows selection of the desired work areas.

- Command Bar – is an area at the top of every form which provides users different actions that can be taken on the form (save, save and close, e-mail a link, etc.).
- Refresh – is used to reload the CRIMES views or forms selection after changes have been made and will allow the user to see the new information.
- Dashboard – the main area where users see role-based inventory and task snapshot.
- Views – in each work area, users can change the displayed data by selecting a different view. Using the view selector, users can select views that will display dynamic data for numerous records (complaints lapse days, administrative cases referred in current FY, etc.).
- Pin – is a tool that allows users to default to a specific view.
- Filter – is a tool on a view that allows users to select certain records.
- Sub-grid – are separate areas on a view that give related information of the view.
- Charts – each view can be displayed as a chart, which gives a graphical representation of selected data fields (by division, group or agent, etc.).
- Tiles/Work area – are specific work areas that give users access to other specific areas. For example, the workplace tile, will give users access to other work areas, like dashboards, contacts, intakes, etc.

80.3 Responsibilities.
The accuracy of information entered into CRIMES is critical to OI's mission. The following are several purposes for which this information is used by OI:

- Managing of case inventory;
- Formulating and justifying OI's annual budget request;
- Determining resource needs for the various OI components;
- Providing statistical data used in Semiannual Reports to the Congress, trend analysis, and testimony given by the Inspector General (IG); and
- Responding to requests for information from entities such as the Secretary of the Treasury, the Commissioner of Internal Revenue, the Government Accountability Office (GAO), the Office of Management and Budget (OMB), and Congress.

In order to ensure that information contained in CRIMES is valid, it is imperative that all data is entered into CRIMES in an accurate, complete and timely manner.

The special agent (SA) is **responsible** for **entering** all relevant data into CRIMES in an accurate, complete and timely manner.

The Assistant Special Agent in Charge (ASAC)/Assistant Director (AD) is **responsible** for **reviewing** CRIMES and **validating** the completeness and accuracy of data entered

into CRIMES. The ASAC/AD is responsible for intake and ensuring case records are properly processed in CRIMES.

The Special Agent in Charge (SAC)/Director will establish procedures whereby they can periodically monitor data entered into CRIMES by personnel in their respective Division to ensure the accuracy of the data. The SAC/Director is responsible for **approving** all records closed to file and all cases in CRIMES. The SAC/Director is **accountable** for the accuracy, completeness, and timeliness of all data entered into CRIMES by the staff in their respective Division.

80.4 Intake/Case Numbering and Information Retrieval Systems.
The numbering system in CRIMES is a uniform method of identifying, controlling, and accounting for intake (complaint, congressional complaint, or lead) and investigation records nationwide. The record number is a series of 10 digits and an alpha definer arranged as follows:

00	0000	0000	XX
Division	Year/Month	Sequence	Alpha Definer

The first 2 digits indicate the Division initiating the record (complaint, congressional complaint, lead, or case).

The 3rd and 4th digits of the series indicate the calendar year and the 5th and 6th digits indicate the month of the record initiation.

The 7th through 10th digits indicate the sequence number of the record, in the order of initiation during the particular month and year.

The 11th digit is either a “C” for complaint, “I” for investigation, or “L” for lead. When congressional complaints are received, the 11th and 12th digits will be “CG” to identify all congressional inquiries.

As an example, the number 55-1701-9999-I indicates:

- Investigation opened by the Operations (OPS) Division in January 2017; and the
- Investigation was the 9,999th investigation initiated by OPS that month.

80.4.1 TIGTA Reference Number (TRN). When a complaint is input into CRIMES, a TRN is automatically generated, which is a system generated number, TRN-XXXX-XXXX and follows a similar numbering system as the complaint.

The first 2 digits indicate the calendar year and the next 2 digits indicate the month.

The last 4 digits indicate the sequential number auto generated by the system during the particular year and month.

Note: When an e-mail address is part of the original complainant contact card at the time of the complaint intake, the TRN is automatically e-mailed to the original complainant. If there is no e-mail on the contact at the time of the complaint intake, the user is responsible for contacting the complainant and providing them the TRN.

80.5 Workplace Area.
Workplace is accessed from the navigation bar and provides users with a centralized area to manage inventory, conduct research, create new records, and track performance on work products. Workplace is divided into the following sub-areas:

- Dashboards;
- Contacts;
- Intake;
- Initiative Requests;
- Cases;
- IMIS;
- Case Plans;
- Case Plan Activities; and
- Reports.

80.5.1 Dashboards. Dashboards provide a role based snapshot of the user's inventory, time and tasks. Sub-grids within the dashboard provide hyperlinks to other parts of CRIMES so that inventory and tasks can be managed in a timely fashion.

80.5.2 Contacts. Contacts provides a centralized index of any person or entity that is the complainant, source or subject of an intake or investigation. Contact records have tabbed information categories that store basic identifiable information; an indices tab that provides hyperlinks to other intake and investigations related to the contact; and a Treasury Integrated Management Information System (TIMIS) tab that allows users to see all historical employment information on Internal Revenue Service (IRS) employees.

Users must conduct an indices search of contacts for a known complainant, source or subject. Users will create a new contact if their indices search of existing contacts does not yield a match. To create a new contact, users are required to input a first name, last name, and an employment status.

Upon review of or input of the contact, users are required to "follow" the contact before making a new intake directly from the contact. This process automatically attaches the details of the contact card onto the new intake allowing easy review of the related

records and historical contact information. If the system detects there is an open record in CRIMES involving the subject or complainant, a banner will flag the intake, alerting the user to review the other open inventory record(s).

If the complainant, source or subject are unknown, users should search and follow the unknown employee or non-employee contact. If the subject is unknown, the user will be required to title the intake. See Section 240. If the subject is a corporate entity, enter the name of the company.

"Confidential Informant/Sources" are contacts stored in CRIMES and maintained by the National Undercover Program Manager. When the original complainant is a formally numbered TIGTA Confidential Source (CS), the user should use the appropriate CS Contact. A system generated reminder will populate in the basis reminding the user to refer to the complainant as CS. Refer to Section 150.3 for additional information related to CS requirements.

80.5.2.1 Contacts Command Bar. The contacts command bar will give users the option to conduct an advanced indices search. By selecting this search option, a report will open that will allow the user to search CRIMES using specific criteria.

80.5.3 Intake. An intake is any complaint, lead or congressional inquiry. Information developed from internal initiatives, integrity projects, or spin-off cases will be documented as leads from the CRIMES case screen. **Complaints received from Congress (committee/member) can only be input by the Operations Division, Policy Team.**

The owner/recipient of the intake is responsible for entering and updating CRIMES data in an accurate, complete and timely manner. System views allow each user to easily track the timeliness and status of intakes, so inventory can be properly managed.

Upon adding a new intake, CRIMES will automatically create a SharePoint (SP) folder. A hyperlink to the folder will be embedded on the Intake record where the following documents and work products are to be stored:

- Memorandum of Interview or Activity (Form OI 2028-M);
- Complaint Referral Memoranda (Forms OI 2070 and 2070-A);
- The written complaint; and
- Any documentation provided in support of the Complaint, to include the scanned document(s).

80.5.3.1 Intake Record Retention. The CRIMES SP folder is the only location where official electronic intake records are to be maintained. Division SP folders should not be used to store or maintain intake records.

Mandatory fields are marked with a red asterisk. Other fields may be required during processing which should generate a system error message indicating what additional information is needed to proceed.

80.5.3.2 Intake Command Bar. The intake command bar provides users access to the following features:

- Clone – allows users an easy way to create complaints that are received from a single complainant but involve more than one subject. After creating the initial complaint, the user will select clone from the intake command bar, which will open a new complaint form which populates all the initial complaint details, but leaves the subject blank. The user adds the additional subject information, updates the basis, then saves the record, which creates a new, and separate complaint and SP folder in CRIMES.

- Ghost – allows users to request sensitive intake records be hidden from any users not in the user's direct chain of command.

- Form OI 6501 – the Form OI 6501, Chronological Case Worksheet feature allows users to create a system generated Form OI 6501 to track intake processing activities. The system stores the Form OI 6501 and provides the user a snapshot of all associated intake activities. When adding intake activities to the Form OI 6501, users will have the option to have a system generated Form OI 2028-M, from CRIMES which will then be automatically stored in the intake SP folder.

  If the complaint is bridged to a case, the Form OI 6501 created on the intake and all the documented activities will migrate with the case. See Section 250.

  Note: Users assisting the SA, through a RAF for example, will also be granted permissions to document the Form OI 6501 related to the support provided and be able to create associated memoranda.

- Extension Request – when users are assigned a congressional, a response date will appear on the intake and case, if created. If users are not able to complete the congressional in the prescribed period of time, they will request an extension from the intake command bar. This request will route to the user's chain of command, then route to the Operations Division for review. See Section 240.

- Charge time – the charge time feature allows users a way to quickly document the hours spent processing an intake. By selecting this feature from the command bar, a new time entry form populates with the intake number, and defaults with the date and the complaint processing activity code. The user will be required to add the hours and a description if applicable. When the time entry

is saved and closed it is automatically associated to the correct pay period and time summary. If the intake is still open, the approved hours will show on the "Hrs Worked In Open" area on the intake form.

- Run Report – users will use this command to create the following system generated documents and are required to store these documents in the CRIMES SP folder associated to the intake:

    - Form OI 2028-M;
    - Forms OI 2070 and 2070-A; and
    - Complaint Tracking Card.

80.5.3.3 CRIMES Intake Form. On the intake form users will see these various tabs:

- Intake Details/Subject & Complainant Info;
- Cross Index/Aliases & RAFS/Spec Techs;
- Narrative; and
- Input by.

The title and status tab contains the title of the intake and the current status. When this tab is expanded it displays the subject, complainant and source contact, basic and detailed information about the complaint including the violation code, allegation received date, if the complainant has been interviewed and the basis narrative and owner information.

The basis must start with the date the allegation was received, who made the complaint (original complainant), the named subject of the complaint and the nature of the allegations. If the complainant did not waive confidentiality or is a CS, CRIMES will flag the intake and provide a reminder in the basis that the complainant should be identified as "T-1" or "CS," as appropriate.

When the user is finished processing the Intake, they will navigate to the intake basics tab to make a referral recommendation and to select which office should receive the referral. See Section 240. The referral recommendations are as follows:

- Transfer;
- Refer for action;
- Refer for info;
- Closed associated with existing case;
- Closed associated with existing intake;
- Initiate investigation; or
- Close to file.

Transfer – used to move an Intake to another group within area of responsibility, or outside area of responsibility.

Refer for Action – this referral is sent to the appropriate IRS or TIGTA. adjudicating office and requires a response indicating the administrative action taken. **Only complaints identifying named employees should be sent for action.**

Refer for Info – this referral is sent to the appropriate IRS or TIGTA adjudicating office and does not require a response from that office.

Closed Associated with Existing Case – used to close a current complaint that involves similar allegations to an existing case.

Closed Associated with Existing Intake – used to close a current complaint that involves similar allegations to an existing intake.

Initiate Investigation – used to close the intake and bridge into an investigation.

Close to file – used when no referral or action can be taken.

Users must be consistent when making the referral recommendation and assure they are preparing the correct referral memorandum. For example, if the user selects refer for information only, a Form OI 2070-A should be completed. Once a referral recommendation is selected, a new option will appear in the command bar as “refer to manager,” which will then create an approval task for the ASAC/AD.

To ensure the accuracy of the intake, the manager will review the referral documents and confirm the recommendation is accurate; and review the data in the intake tab and work areas to ensure the completeness and accuracy of the entries before approving the task.

If the manager approves the task, but later determines the information is inaccurate, or it is decided by the SAC/Director that adjustments are required, the ASAC/AD or SAC/Director will follow the user guide on how to reactivate and update the Intake record.

The “Intake Details/Subject & Complainant Info” tab is also where the intake status and dates are shown and the personally identifiable details for the subject and complainant. Updates to personally identifiable information involving the subject or complainant should be made from this section which will update the contact card.

Confidentiality **ONLY** applies to an IRS, TIGTA, or Treasury employee, as such the field for confidentiality waived will only appear if the complainant is an IRS, TIGTA or Treasury employee.

The "Cross Index/Aliases & RAFS/Spec Techs" tab is where users add cross indexes, aliases; where users make system generated requests to specialized support divisions and track specialized techniques used when processing the complaint.

The "Narrative tab" is where users will view and edit the basis, results and remarks. Results and remarks are not mandatory fields for intakes. Users will add miscellaneous and discretionary information relating to the intake in the remarks narrative section. If the complaint is bridged to an investigation, the narrative fields, including the remarks will migrate to the investigations remarks section. Therefore, a review of the remarks should be made to insure all information is germane to the investigation.

The "Input By" tab shows who created the intake record.

80.5.3.4 Other Intake Work areas. From the navigation bar, the intake record has other related work areas where other information is stored separately including the following:

- Activities;
- Violations;
- Referrals;
- Connections;
- Time Entries;
- Manual Share; and
- Audit History.

Activities – allows users to see where related tasks are in the workflow process. Users should review this area when they want to know who has an open task or when a task was processed.

Violations – allows users to input additional violation codes. The primary violation code should be set from the main intake screen. Prior to referring an intake, the violations should be reviewed to ensure duplicates are not listed.

Referrals – is used to track and store the administrative referrals and actions. All administrative results should be entered in an accurate, complete and timely fashion.

Connections – displays other intake records created during the clone process.

Time Entries – displays the time entries for a specific intake.

Manual Share – allows users to allow read and write access for the intake, SP folder, or both to their trainers and others assisting in processing the intake.

Audit History – provides details about when and whom made changes to the intake record.

Intake Views – users will navigate to the intake work area and change the view to see system views or personally created views that will assist in managing their inventory. Two of these views which can assist in ensuring timeliness are:

- Complaints Lapse Days; and
- Complaints Open.

Note: Information developed from internal initiatives, such as the Strategic Data Services (SDS) unauthorized access (UNAX) detection efforts, Office of Audit (OA) referrals, integrity projects, or leads on additional subjects **should only be created from the master case** using the "Create a Lead" option on the command bar.

80.5.4 Initiative Requests. Users will navigate to initiative requests to make a request for approval regarding a LII or NII.

The requestor will complete a new initiative request form, indicating the title describing the initiative, a violation and statute, a brief basis, the investigative steps and the goals of the initiative. If seeking approval for an initiative that does not require approval from the Integrity Board, such as remittance testing, the requestor should select "Reoccurring LII or NII," which will route approvals through their chain-of-command. Once the initiative is approved, a case can be initiated by selecting initiate case on the command bar.

80.5.5 Cases. The Cases area stores all investigation records.

80.5.5.1 Cases Command Bar. The Case Command Bar gives users access to the following features:

- Ghost;
- Create lead;
- Form OI 6501 ("6501");
- Extension request (if CG)
- Charge time; and
- Run report.

Ghost – allows users to request sensitive case records be hidden from any users not in the user's direct chain-of-command.

Form OI 6501 – the Form OI 6501 feature allows users to create a system generated Form OI 6501 to track intake processing activities. The system stores the Form OI 6501 and provides the user a snapshot of all associated intake activities. When adding intake activities, users will have the option to have a system generated Form OI 2028-M, from CRIMES which will then be automatically stored in the intake SP folder.

Note: If the Form OI 6501 was created on an intake that is bridged to a case, it will migrate to the case.

Users assisting the SA, through a RAF for example, will be granted permissions to document the Form OI 6501 with the support provided; and create and save associated memoranda in the SP folder.

Extension Request – when users are assigned a congressional, a response date will appear on the case. If users are not able to complete the congressional in the prescribed period of time, they will request an extension from the case command bar. This request will route to the user's chain of command, then route to Operations Division for review and to the appropriate DAIGI for approval. See Section 240.

Charge Time – the Charge time feature allows users a way to quickly document the hours spent processing a case. By selecting this feature, a new time entry form populates with the case number, and defaults with the date and the investigation processing activity code. The user will be required to add the hours and a description, if applicable. When the time entry is saved and closed it is automatically associated to the correct time summary. If the case is still open, the approved hours will show on the "Hrs Worked in Open" field on the Case form.

Run Report – users will use this command to create the following system generated documents and are required to store these documents in the CRIMES SP folder associated to the case:

- Referral Forms OI 2028R, 2076, 2076PDT, 2076PDTU;
- Form OI 2028-M
- Form OI 8273, Assault, Threat, Threat Assessment, and Harassment Incident Report; and
- Investigation Card.

80.5.5.2 Case Form. The Case form offers the user various tabs, including:

- Details/Subject and Complainant Info;
- Case Dates;
- Rights, Representation & RAFS;
- Cross Index, Aliases & Evidence;
- Related Cases and Intake;
- Narrative; and
- Records Control and Disposal.

The title and status tab contains the title of the case and the status. When expanded, it will provide the subject, complainant and source contact, basic and detailed information about the case including the primary violation code, allegation received date, if the complainant has been interviewed, the basis narrative and owner information.

SAs will navigate to this section when they are finished processing the complaint to add a referral recommendation. In doing so, a new command option will appear that will allow them to refer to their manager which will then create an approval task which is e-mailed to their ASAC/AD.

To make a strictly administrative referral the user will select “Refer for Information” or “Refer for Action.”

To add a criminal referral, users will select “Make a Criminal Referral” and document whether the referral is pending, accepted or declined. The system will require there be a named subject and at least one initiation statute input for the case. It will also require users to add where (*e.g.,* Assistant United States Attorney, Department of Justice-Tax Division) the criminal referral is being made, the referral date and the judicial district.

In order to document a referral to a State/Local prosecutor in CRIMES, a referral to a Federal prosecutor and subsequent declination must be documented first. See Section 70.5, for additional information on prosecutive referrals.

If adding a referral that was declined for prosecution the user will be required to document the reason. If the reason for the declination is a Blanket Declination Agreement (BDA), the current BDA covering the referred violation should be uploaded to the case SP folder.

If the referral has been accepted for prosecution, users will be required to add the date accepted and the first legal action. This will also be when the user will identify whether the subject is a fugitive. By selecting “Yes,” the system will require the date National Criminal Information Center (NCIC) was verified and the NCIC number. There will also be a banner on the case and the subject’s contact card.

Details/Subject and Complainant Info – this tab is where the case dates are shown and the personally identifiable details for the subject and complainant. Updates to personally identifiable details involving the subject or complainant should be made from this section which will update the contact card.

Case Dates – shows a quick way to look at important case dates, such as when the allegation was received, which is the date the allegation was received by TIGTA or the sentencing date, as examples.

Rights, Representation & RAFS – this tab provides a sub-grid where users are required to document what administrative or criminal warnings were administered during the subject interview and who accompanied the subject at the time they were interviewed.

There is a separate sub-grid where users will make RAF requests for assistance from:

- Operations Division/IG Subpoena;
- Collateral requests from other Divisions;
- SDS;
- Technical and Firearms Support Division (TFSD);
- Criminal Intelligence & Counterterrorism Division (CICD); and/or
- Forensic & Digital Science Laboratory (FDSL).

Users will also add specialized techniques executed under the authority of OI or specialized equipment and techniques in this section such as surveillance, shotgun, and search warrant.

Note: If working a joint investigation with another Federal agency and the other Federal agency applies for and obtains a search warrant, CRIMES would be documented as Code 30 – Other Agency Specialized Technique, not Code 10 – Search Warrant, as it was not obtained or executed under the authority of OI.

To document an "IRS Examination Referral" users should select this specialized technique and ensure the Exam Referral Form 8109 EMP or 8109NE has been prepared and uploaded to the CRIMES investigation SP folder. Use of this specialized technique requires that one of the case violation codes be Violation Code 718 – Willfully Understates Federal Tax Liability. After saving and closing this specialized technique form, an approval will be required by the manager. Once approved, the IRS exam referral date will appear in the case details tab. **Upon the return of the exam results, the user should navigate to this tab and enter the date returned by the IRS.**

Cross Index, Aliases & Evidence – this tab provides sub-grids where users add individuals and entities that are substantively involved in the investigation. Persons merely providing records, such as a records clerk at a police department, or individuals forwarding or facilitating the flow of information to TIGTA, such as an employee of the IRS Employee Conduct and Compliance Office, should not be cross-indexed to the investigation.

The alias sub-grid should be used to document other names that may be used, or have been used by the subject or complainant, including a business or other types of entities that are closely associated.

Evidence obtained for a case must be documented in the case evidence sub-grid in CRIMES. See Section 190.

Related Cases and Intake – provides sub-grids that show if the case is a master or spin off and which intake it was associated to. Leads and other spin off cases will also be shown here.

This is also where users will find the joint investigations sub grid. If a case is being worked jointly with another agency the agent is required to identify the agency and the agency's case number.

Narrative – is where users will view and edit the basis, results and remarks sections. The basis must match verbatim the first paragraph of the investigative synopsis section of Form OI 2028R. The results are a brief synopsis of what is documented in the remaining paragraphs from the investigative synopsis section of Form OI 2028R. Remarks are not a mandatory field. Users will add miscellaneous and discretionary information relating to the case in the remarks narrative section. The narrative should be a synopsis and not a duplicate of the initiating Form OI 2028-M, Memorandum of Interview or Activity.

Records Control and Disposal – is where support staff document that the hardcopy investigative file has been forwarded from the divisional field office to the Operations Division's Records Management Section (RMS). Upon receipt of the file, RMS will add the date received to the case record tab. Other RMS dates and record retention information is also stored here.

80.5.5.3 Other Case Information. Like intake, other relevant case information is stored separately on related case entities, which are accessible from the case navigation bar. Those areas unique to a case are as follows:

- Activities;
- Referrals;
- Inv Violations;

- Inv Statutes;
- Inv Financial Info;
- Inv Sensitivity;
- Time Entries;
- Manual Share; and
- Audit History.

Activities – allows users to see where related tasks are in the workflow process. Users should review this area when they want to know who has an open task or when a task was processed.

Referrals – is where users will add updates to administrative or criminal referrals. Adding information to a criminal referral will lead to updating associated statutes, financial recoveries and sentencing information.

Note: Financial recovery information should not be counted more than once in CRIMES. For example, if three individuals conspired to defraud the government of $10,000, then the $10,000 theft, or attempted theft would not be documented under each of the three investigations, as this would add up to $30,000. Instead, the $10,000 would be documented within only one of the investigations, or allocated evenly between the three related investigations. If necessary, additional remarks may be made in the remarks section to further explain the division of financial recoveries between the related cases.

Inv Violations – this is where additional violation codes will be added. The primary violation is updated from the case form, not in this this area. If duplicates are listed in this area, they must be removed prior to referring the case for adjudication or an alert notice will not be sent to the IRS.

Inv Statutes – is where additional initiation statutes are added ONLY; the legal action and conviction statutes will be added during other parts of the referral process.

Inv Financial Info – is where non-legal action financial codes are added.

Inv Sensitivity – is used to document the sensitivity codes, particularly when there is:

- Source of, or interest by, high-level Government entities;
- Sensitivity of the particular type of violation; or
- Investigations being worked jointly with other agencies.

Time Entries – shows the time entries on a specific case.

Manual Share – allows users to grant read and write access for the case, SP folder, or both to their trainers and others assisting in processing the case.

Audit History – provides details about when and whom made changes to the case.

80.5.6 Investigations Management Information System (IMIS). Users will search this area to gather basic information from the legacy IMIS which was the management information system used by IRS Inspection/TIGTA.

80.5.7 Case Plans and Case Plan Activities. Case Plans is a central work area that allows all users a quick way to access their case plans and review activities.

80.5.8 Reports. Reports provides users a way to help manage the agency performance goals.

80.6 Activities.
Activities is another primary work area in CRIMES which includes the following categories:

- Outreach – is used to track post-of-duty visitations and awareness presentations;
- Acting & assignments – is where acting privileges are created and where intake and case records can be reactivated and deactivated; and
- Records Management – provides records retention information; used primarily by support staff and the RMS.

80.7 Time Management.
The time management work area is accessed from the navigation bar, and is divided into two categories:

- Time summary – stores all users time summaries; and
- Time entries – stores every time entry.

Time summary is where users should navigate to create or edit time for a particular pay period.

80.8 Request Assistance Forms (RAFS).
RAFS are system generated requests for specialized support. This area allows users to view all open, requested and inactive RAFS.

80.9 Help.
The CRIMES help area can be accessed from the navigation bar, and is divided into the following categories:

- CRMS Help; and
- Guide/FAQs.

80.9.1 CRMS Help. The purpose of the CRMS Help area is to provide a built in mechanism for users to request assistance with CRIMES functionality and to suggest modifications in future deployments of the system.

80.9.2 Help Guide/FAQs. The purpose of the Help Guide/FAQs function is to link users to the SP site for CRIMES where the entire user guide is stored, searchable and downloadable.

DATE: July 1, 2018

CHAPTER 400 - INVESTIGATIONS

(400)-90 Occupational Health, Safety, and Wellness

90.1 Overview.
This section includes the following information related to the Occupational Health, Safety, and Wellness program for the Office of Investigations (OI), and includes the following:

- Health Improvement Program (HIP)
- Official Time
- Responsibilities
- Occupational Exposure to Bloodborne Pathogens (BBPs)
- Confidentiality and Record-Keeping

The U.S. Congress and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) recognize that due to the nature of a special agent's (SA's) occupation, there is a need for established physical requirements and recommends that agencies assist SAs by offering them a fitness program. Title 5 U.S.C. § 7901, authorizes agencies to establish a health service program to promote and maintain the physical and mental fitness of their employees.

This CIGIE physical capabilities guideline has been incorporated within two areas of OI's Occupational Health, Safety, and Wellness Program: The Health Improvement Program (HIP) and the Occupational Exposure to Bloodborne Pathogens (BBPs). The foregoing information pertains to OI's Occupational Health, Safety, and Wellness Program and does not establish or supersede Agency-approved medical standards.

90.1.1 Acronyms Table.

90.2 Health Improvement Program (HIP).
In order to promote wellness and help all SAs meet job-related medical standards and physical requirements, a voluntary physical fitness program for all GS-1811s, Criminal Investigators/SAs was established. The objectives of the HIP are to improve and maintain the fitness level of SAs, encourage life-style changes that will increase wellness and productivity, and decrease disability within the workforce. Proper physical conditioning for SAs is essential to enable them to meet the physical demands of their law enforcement position.

The HIP is voluntary and encourages SAs to engage in approved health and fitness improvement/maintenance program activities. It grants approval to use official time while performing approved HIP activities. In order to participate in the program, SAs must stay in compliance with the following requirements:

- Participate in and complete an annual fitness assessment, administered by a trained HIP coordinator; and
- When notified by a HIP coordinator of an upcoming clearance expiration, schedule and complete the annual health and medical screening, and obtain a subsequent clearance status in a timely manner. Health clearances expire one year after issuance.

If an SA has not been medically cleared, and has not participated in the fitness assessment, he/she may not charge official time to the HIP program.

It is the responsibility of every HIP-participating SA, their manager, and HIP coordinators to abide by the rules established for the HIP in order to ensure that the program is safe and mutually beneficial to SAs and OI. In addition, all records associated with the HIP program will be maintained in accordance with provisions of the Privacy Act.

90.2.1 Medical Screening/Clearance. Each HIP-participating SA will undergo an initial and annual medical screenings. The OI trained HIP coordinator will contact the SA and inform them of the requirement to obtain a medical screening, which will be conducted by a medical provider with Federal Occupational Health (FOH) or a private physician. If a private physician is used for an annual HIP screening, the SA is responsible for all associated expenses. Pre-employment screenings are required to be conducted by FOH. If private physicians are used, they are required to follow the same screening guidelines as an FOH physician. The private physician must submit documentation to FOH for a medical review and subsequent clearance. The required medical screenings will include at a minimum:

- Completion of TIGTA's FOH-5 (Short Form), *Health History and Physical Examination Form*;
- Blood analysis; and
- Blood pressure check.

HIP medical screenings expire one year from the date the SA is deemed medically cleared by an FOH physician. Medical clearance dates are reported on the *Medical Review Form* provided by FOH. HIP coordinators do not have a need to know an SA's specific health information. The Federal Law Enforcement Training Center (FLETC) is responsible for medically clearing SAs prior to attending basic training programs, and as required for other training programs. For SAs who have recently attended and graduated from FLETC's Criminal Investigator Training Program, or its equivalent, their HIP medical clearance expires one year from the date they initially began the training program.

It is the responsibility of the local or divisional HIP coordinator (if no local coordinator is appointed) to notify participating SAs 60 days in advance of their clearance expiration date and provide them with guidance on how to renew their participation. Participating SAs are required to schedule medical screenings as soon as possible to avoid unnecessary delay, which could cause a lapse in their medical clearance.

The HIP coordinator shall immediately notify the participating SA's manager when the SA's medical clearance date is received (to include the expiration date), anytime there is a lapse in an SA's medical clearance, or an SA's medical clearance is denied.

Any restrictions on an SA's ability to participate will be determined by FOH, who will notify the appropriate HIP coordinator. In such cases where an SA opts to utilize a private physician, FOH will work with the private physician to medically clear the SA, as appropriate.

Under no circumstances should a HIP coordinator or manager request to see an SA's medical information for the purpose of participating in the HIP program.

90.2.2 Physical Fitness Assessments. After the medical screening and a subsequent medical clearance is obtained, each SA will participate in a physical fitness assessment conducted by a trained HIP coordinator. The focus of the assessment is to measure:

- Cardiorespiratory fitness;
- Abdominal muscular endurance; and
- Muscular endurance.

90.2.2.1 Approved Physical Fitness Assessment. Physical fitness assessments are an annual requirement for any medically cleared SA wishing to participate in the HIP. Prior to administering the assessment, the HIP coordinator will obtain verbal confirmation from each participating SA indicating if he/she feels well to participate in the assessment. The SA's verbal response shall be documented on the Fitness Assessment Record. See Exhibit (400)-90.3.

A first aid kit and directions, to include phone number(s), to the nearest hospital or other adequate medical facility that is readily accessible must be available during the fitness assessment. OI's approved assessment is consistent with the Cooper Standards and is outlined below:

- 1.5 mile run;
- Sit-up test; and
- Push-up test.

This is the only authorized assessment to be administered, and no deviations from this assessment are authorized. Only OI trained HIP coordinators may administer the approved physical fitness assessment. See Exhibit (400)-90.1.

The HIP coordinator administering the assessment will record SAs' results on the *Fitness Assessment Record*. See Exhibit (400)-90.3. The HIP coordinator shall also refer participating SAs to the Cooper Standards Scoring Table, if desired. See Exhibit (400)-90.2. If an individual is unable to participate in a scheduled fitness assessment because of a temporary injury, he/she will, after a rehabilitation period, attempt to participate in a subsequent fitness assessment. SAs will not be permitted to charge time to the HIP until they have successfully completed the assessment.

90.2.2.2 Authorized Program Activities. Authorized physical fitness activities for the HIP are those recognized by OI for coverage under the Federal Employees Compensation Act (FECA) during the three hours of official time authorized per week, to participate in the HIP. See Section 90.3. SAs are not covered under FECA when performing these activities while in a non-pay status. Approved activities are those that address one or more of the following areas of fitness:

- Aerobic capacity;
- Flexibility;
- Muscular endurance; and/or
- Strength.

The following fitness activities are authorized by OI:

- Brisk Walking;
- Jogging;
- Running (stationary or outdoor);
- Cycling (stationary or outdoor);
- Cross-country skiing;
- Treadmill;
- Stair climbing/stairmaster;
- Elliptical cross-training machine;
- Rowing;
- Swimming;
- Aerobic classes;
- CrossFit;
- Rope skipping;
- Strength/resistance exercises (such as weight training, including the use of free weights, calisthenics, etc.); and/or
- Flexibility exercises (such as stretching, yoga, pilates, etc.).

90.3 Official Time.
SAs are authorized three hours per week of official time to engage in approved fitness activities, whether during the normal workday, before or after the workday, or on weekends. Of the allotted three hours, SAs may take no less than a half hour and no more than one and a half hours on a single day. There is no accumulation of unused hours; therefore, hours cannot be carried over from week to week. The authorized three hours includes pre and post-workout activities (*e.g.*, stretching, showering).

SAs who use official time during their regular tour of duty must obtain pre-approval from their manager and keep them informed of their location.

Approved fitness activities engaged in outside of the regular workday, may be recorded as official time for the purposes of Law Enforcement Availability Pay (LEAP). Compensatory time or overtime will not be utilized for fitness activities. Official time for fitness activities cannot be taken on days in which all other hours are recorded as leave.

SAs are permitted to use a government-owned or leased vehicle to drive a reasonable distance to a fitness facility/area before or after a scheduled workday, as well as on the weekends. Driving time shall not be included in HIP official time. Questions regarding the reasonableness of the distance between the fitness facility/area and the SA's residence, temporary duty location, or post of duty (POD) should be addressed by the SA's manager, as appropriate.

SAs not receiving LEAP (*i.e.*, employees engaged in the Special Agent Part Time Employment Program, etc.) may only participate in the HIP during their official tour of duty hours. See Chapter 600, Mission Support, Section 70.22 of the TIGTA Operations Manual.

90.4 Responsibilities.
This section addresses the responsibilities of the HIP program.

90.4.1 National HIP Coordinator Responsibilities. The national HIP coordinator is responsible for the overall management of OI's HIP, the program's budget, as well as all the duties expected of a contracting officer's representative. These duties of the national HIP coordinator include, but are not limited to:

- Review and audit invoices from vendors such as FOH for accuracy and advise vendors of any discrepancies;
- Serve as a liaison between vendors, including contracted psychologists, HIP coordinators, the Bureau of Fiscal Services, contracting officers, and the Office of Mission Support, as needed;
- Track fitness-for-duty examinations;
- Maintain a list of HIP coordinators and training each coordinator has received;

- Coordinate training for divisional and local HIP coordinators;
- Maintain and update the list of TIGTA SAs and their respective local and divisional coordinators, and ensure vendor for HIP has a current list; and
- Manage the BBP Program, including Exposure Control Plan.

90.4.2 Divisional HIP Coordinator Responsibilities. The divisional HIP coordinator is responsible for duties that include, but are not limited to:

- Ensure SAs within their division have all medical information submitted to and tests conducted timely by FOH;
- Annually offer the hepatitis B vaccinations to all SAs. See Exhibit (400)-90.4;
- Maintain an updated list of local HIP coordinators and the HIP-participating SAs within their division, and advising the national HIP coordinator of changes;
- Serve as the primary division point-of-contact for FOH personnel;
- Inform the national HIP coordinator of any divisional issues concerning the HIP or BBP programs;
- Ensure that each SA in his/her division complete the annual BBP training course in the Integrated Talent Management System;
- Coordinate and ensure all SAs within their division maintain active cardio-pulmonary resuscitation (CPR) certification and first aid training; and
- Assume the duties and responsibilities of the local HIP coordinator in those PODs where no local coordinator is available.

90.4.3 Local HIP Coordinator Responsibilities. A local HIP coordinator is assigned to a group within OI, where available, and is responsible for duties that include, but are not limited to:

- Ensure that all medical screenings and assessment results are received which show the SA is approved to participate in the HIP;
- Maintain records of an SA's FOH clearance status;
- Administer annual fitness assessments;
- Maintain all fitness/clearance information for all SAs in a locked, secure file cabinet or safe;
- Document time spent on above activities in the Criminal Results Management System (CRIMES) Time Report, utilizing Activity Code "81-HIP Coordinator Duties;" and
- Encourage and supporting SAs in achieving their fitness goals by developing appropriate fitness plans, as requested.

HIP coordinators are permitted to disclose clearance status information only as authorized by law, including to HIP and/or FOH personnel, who have a need-to-know. HIP coordinators must promptly notify managers of any safety-related concerns or failure to obtain clearance.

90.4.4 Manager Responsibilities. Each manager's responsibilities include, but are not limited to:

- Discuss the HIP with each SA and ensure SAs keep him/her informed of the location and time of fitness activities during the workday;
- Ensure HIP time is properly documented in the CRIMES Time Management Report, utilizing Activity Code "82-HIP Approved Individual Activities," and that time claimed on one day is not less than a half hour and does not exceed an hour and a half, and ensuring total hours claimed in one week do not exceed three hours;
- Identify and discuss with SAs when official duties will preempt pre-approved HIP activities;
- Upon request, referring an SA who requests assistance with developing a plan for his/her individual fitness activities, to a HIP coordinator; and
- Ensure SAs who claim HIP time are cleared annually by FOH. SAs' clearance status will be sent to the manager by the local or divisional HIP coordinator when it is received by FOH.

90.4.5 SA Responsibilities. Each SA's responsibilities include, but are not limited to:

- Undergo an initial and annual medical screening and physical assessment;
- Track the expiration of his/her annual medical clearance;
- Notify his/her HIP coordinator of any changes to health that may affect his/her current level of participation in the HIP. Some conditions, such as pregnancy, may require a note from a physician, which specifies the activities the SA is able to continue performing;
- Participate in an annual fitness assessment;
- Communicate fitness needs and goals to the HIP coordinator, as appropriate;
- Ensure his/her manager is informed of his/her location during participation in approved health and fitness activities during a regular tour of duty;
- Document HIP activities in CRIMES Time Report, utilizing Activity Code "82-HIP Approved Individual Activities," and entering the specific HIP activity conducted (*e.g.*, brisk walking, running, weight training) in the comments section of the report; and
- Ensure that not less than a half hour and not more than an hour and a half of official time is claimed on one day, and not more than three hours is claimed in one week.

90.5 Occupational Exposure to BBPs.
The Occupational Safety and Health Administration (OSHA), 29 C.F.R.§ 1910.1030, Occupational Safety and Health Standards, outlines regulations concerning the protection of employees from exposure to blood or other potentially infectious materials.

This OSHA regulation applies to all employees who may receive occupational exposure to blood or other potentially infectious materials in the course of their official duties.

For employees with occupational exposure, as defined by OSHA regulations, TIGTA is required to:

- Establish an Exposure Control Plan and Exposure Determination for employees with an occupational exposure;
- Provide training in accordance with the OSHA standards; and
- Maintain medical and training records, as appropriate.

90.5.1 Occupational Exposure Determination. OSHA defines employee occupational exposure as, “reasonably anticipated skin, eye, mucous membrane, or parenteral contact with blood or other potentially infectious materials that may result from the performance of an employee’s duties."

Employees at increased risk need to be included in special programs designated by the OSHA BBPs Standard including special training, issuance of personal protective gear (*i.e.*, gloves and eye protection, and voluntary immunization for hepatitis B, etc.). Generally, the normal duties of SAs involve no exposure to blood or body fluids; however, their employment may require the occasional performance of tasks that could result in exposure to blood, tissues, and bodily fluids including, but not limited to:

- Arrests;
- Searches of individuals or property;
- Execution of search warrants;
- Interviews involving potentially hostile individuals; and/or
- Escorting prisoners.

Employees located at the Forensic and Digital Science Laboratory (FDSL) occupying the following job classifications should be mindful that their employment may require the occasional performance of tasks, which could result in exposure to blood, tissues, and/or bodily fluids:

- Series 1397 - Forensic Document Examiner
- Series 0072 - Latent Specialist
- Series 0344 - Management Assistant
- Series 0301 – Evidence Custodian

The tasks FDSL staff may be required to perform include, but are not limited to:

- Examining, documenting, collecting and packaging crime scene evidence;
- Creating graphics demonstration materials for court, trainings, briefings;

- Crime scene processing; and/or
- Providing first aid and/or CPR assistance.

All other OI employees not listed above are considered to have normal duties, which generally do not involve exposure to blood or body fluids, and their employment generally does not require the occasional performance of tasks, that could result in exposure to blood, tissues, and/or bodily fluids.

90.5.2 Exposure Control Plan. The OSHA BBP standard requires an agency with employees who have the potential for an occupational exposure to create a written Exposure Control Plan.

The Exposure Control Plan contains specific elements such as:

- The Exposure Determination that includes a list of job classifications in which employees have occupational exposure, and a list of tasks or procedures when occupational exposure occurs;
- Methods of compliance for exposure prevention;
- Methods of implementing voluntary vaccinations and post-exposure evaluation and follow up;
- Communication of hazards to employees; and
- Record-keeping requirements.

A copy of the Exposure Control Plan must be accessible to employees and updated by the national HIP coordinator, when necessary, to reflect revised tasks and procedures, affecting occupational exposure. A copy of the Exposure Control Plan can be found on OI's intranet site.

90.5.3 Hepatitis B Review and Vaccination. Hepatitis B virus (HBV) is a virus that affects the liver and is transmitted by exposure to blood and other potentially infectious materials. The virus that causes hepatitis B infection is transmitted in various bodily fluids (*e.g.*, saliva). It is most often transmitted in contaminated blood products and via needle puncture wounds. HBV continues to be the most critical occupational hazard for persons exposed to blood or other potentially infectious materials.

There is a preventative HBV vaccine for treatment of personnel both prior to and after exposure to the hepatitis B virus. The first two doses are given one month apart, and the third dose is given five months after the second. Protection for normal, healthy adults and children given the HBV vaccine is believed to last at least 30 years.

The HBV vaccination must be made available to all employees occupationally exposed to blood or other potentially infectious materials on an annual basis, and the responses maintained by the local or divisional HIP coordinator. See Exhibit (400)-90.4.

Law enforcement personnel and others whose duties are to perform tasks involving contact with blood or blood-contaminated body fluid should be vaccinated. However, vaccinations are voluntary.

An employee may opt for a post-exposure vaccination, which is reported to be as effective as a pre-exposure inoculation.

Timely post-exposure management may be considered rather than routine pre-exposure vaccination for law enforcement and other personnel whose exposure to blood or other potentially infectious materials is infrequent.

90.5.4 BBP Training. Upon determination that an employee is likely to have occupational exposure to blood or other infectious materials, regulations require TIGTA to provide appropriate training and counsel prior to or upon receipt of the inoculation.

The OSHA BBP Standard requires initial training with annual updates for employees who are at increased risk for BBP exposure.

90.5.5 Additional OSHA Requirements. The OSHA regulations also contain requirements for post-exposure evaluation and follow up.

90.5.6 Costs. OI will pay all costs for SAs and other OI personnel performing duties determined to be “at risk” to blood or other potentially infectious materials for necessary services including all medical evaluations/procedures, HBV vaccination, vaccination series, and post-exposure and follow up evaluations.

90.6 Confidentiality and Record-Keeping.
Fitness information is subject to the provisions of the Privacy Act and will be maintained in a secure manner. HIP coordinators must not request or maintain any personal health information; and, must ensure that physical and/or electronic FOH clearance information is securely maintained. Copies of bloodwork results or TIGTA's FOH-5 (Short Form) are not authorized to be maintained by HIP coordinators.

90.6.1 Confidentiality. HIP coordinators will have access only to information needed to administer the program. HIP coordinators are authorized to disclose FOH clearance information pertaining to an SA to the SA’s manager and FOH personnel, only on a need to know basis.

All FOH clearance records will be kept confidential and not disclosed or reported to any person within or outside TIGTA without the employee's written consent, except as authorized by a law.

90.6.2 Records. HIP coordinators who have the responsibility of maintaining records will comply with the requirements outlined below:

- Maintain copies of records relating to SA's HIP activity(ies) for a period of three years after the activity is completed or superseded, unless otherwise required to be maintained longer for business purposes, and then they must be destroyed. See guidance outlined in National Archives and Records Administration General Records Schedule (GRS) 2.7: Employee Health and Safety Records;
- Maintain copies of incident records, not medical records, related to occupational exposure of BBPs; and
- These records should be maintained at the local/divisional level until the employee separates from TIGTA, at which time these records shall be forwarded to the national HIP coordinator for appropriate records retention.

DATE: April 1, 2021

CHAPTER 400 - INVESTIGATIONS

(400)-100 Special Agent Training and Professional Development

100.1 Overview.
Special Agents (SA) must possess the knowledge and skills required to perform investigative activities. The Office of Investigations (OI) utilizes its own Treasury Inspector General for Tax Administration (TIGTA) Training Academy (Academy), the Federal Law Enforcement Training Centers (FLETC), and other venues to provide a wide range of formal and informal training as well as professional development opportunities to SAs. OI's training program meets the training guidelines established by the Council of Inspectors General on Integrity and Efficiency (CIGIE).

This section describes the following training programs and activities:

- Academy
- Core Training Programs
- On-the-Job Instructor Training Program
- On-the-Job Training Program
- Advanced Training
- Firearms, Agent Safety, and Tactics Training
- External Training
- Continuing Professional Education
- Leadership Development Program
- Instructor Cadre Program
- Self-Development Activities
- Individual Development Plan
- Training Requests
- Instructor Details to the Federal Law Enforcement Training Centers

Additional information related to TIGTA training not specific to OI is contained in Chapter 600, Section 70.19 of the TIGTA Operations Manual.

100.1.1 Acronym Table.

100.2 Academy.
The Academy staff consists of an Assistant Special Agent in Charge (ASAC), two SAs who serve as course developers, one SA who serves as the National Firearms, Agent Safety, and Tactics Coordinator, a program analyst who serves as the accreditation manager, and a training analyst. The Academy offers four training programs described in this Section.

100.2.1 Accreditation. The Academy is accredited by the Federal Law Enforcement Training Accreditation (FLETA) Board. Additionally, TIGTA's Special Agent Basic Training (SABT) and Special Agent Advanced Training Program (SAATP) are also accredited by FLETA. The accreditation of a Federal law enforcement academy or program provides assurance to the citizens it serves that it voluntarily submitted to a process of self-regulation and successfully achieved compliance with a set of standards collectively established within a professional community of its peers which demonstrate adherence to quality, effectiveness, and integrity.

100.2.2 Integrated Talent Management System. OI utilizes the Integrated Talent Management System (ITMS) to provide employees with professional development. ITMS serves as a tool to assist employees and supervisors with identifying and managing personal career goals, viewing training history, generating training assessment reports, accessing and completing web-based personal development courses through the Skillsoft catalog, and initiating and tracking all requests for external training. Mandatory and elective professional development courses are assigned to OI employees and their completion recorded in ITMS.

100.3 Core Training Programs.
OI has identified four training courses that are essential to the long-term success of every SA and ASAC. Core training includes FLETC's Criminal Investigator Training Program (CITP), SABT, SAATP, and ASAC In-service Training (AIT).

100.3.1 Criminal Investigator Training Program. CITP is a formal training program administered through FLETC in Glynn County, Georgia, and provides instruction in basic law enforcement concepts, skills, and techniques using classroom instruction and hands-on practical exercises.

All SAs must successfully complete CITP or an equivalent training program. CITP should be scheduled as soon as practical and, if possible, prior to attending SABT. Additional details regarding CITP can be found at www.fletc.gov.

100.3.2 Special Agent Basic Training. SABT is a TIGTA-specific training program for new TIGTA SAs. Emphasis is placed on conducting investigations unique to TIGTA. Non-supervisory SAs must attend and successfully complete SABT. Entry-level SAs must be scheduled for SABT as soon as practical after completing CITP. Supervisory SAs that are new to TIGTA will audit SABT as soon as practical.

Professional OI staff (non-SAs) may attend SABT in an audit capacity to enhance their ability to execute their assigned tasks. Participation is limited to positions that directly support and interact with investigations, or would demonstrably benefit OI in some other way. The employee's Special Agent in Charge (SAC) or Director will submit a request for professional staff attendance to their respective executive, and detail how the employee's attendance at SABT will benefit the organization.

Both CITP and SABT are designed to develop the appropriate skills for new SAs related to the following:

- Ethics and professional conduct;
- Criminal and constitutional laws;
- Interviewing, preparing forms, and writing reports;
- Inputting and processing complaints and investigations in TIGTA's Criminal Results Management System;
- Investigative procedures and techniques; and
- Officer safety.

100.3.3 Special Agent Advanced Training Program. SAATP is a TIGTA-specific training program for experienced SAs that provides classroom instruction and hands-on training in advanced investigative concepts, skills, and techniques. All non-supervisory SAs must successfully complete SAATP once every three years.

100.3.4 Assistant Special Agent in Charge In-service Training. The AIT is a TIGTA-specific training program for ASACs that provides classroom instruction and hands-on training in advanced investigative concepts, skills, and techniques. It is desirable that all ASACs successfully complete AIT once every three years.

100.4 On-the-Job Instructor Training Program.
In addition to the required core training programs, the Academy offers specialized training through the On-the-Job Instructor Training Program (OJITP). OJITP provides training to SAs who are On-the-Job Instructors (OJI) for newly-hired SAs.

100.5 On-the-Job Training Program.
The On-the-Job training (OJT) program is a formal process designed to provide new SAs with one-on-one instruction and hands-on experience to develop their knowledge, skills, and techniques in various investigative and administrative matters. All non-supervisory SAs new to OI must successfully complete the OJT program.

The OJT program is implemented locally by the SAC/Director level, but program oversight is the responsibility of the ASAC-Training Team. To assist with implementation of the OJT program, OI utilizes the "TIGTA OI On-the-Job Instructor Training and Performance Evaluation Program" manual (alternatively referred to as the OJT Manual).

OJT includes instruction related to the following:

- Organization, history, and mission of the Internal Revenue Service (IRS) and TIGTA;

- Agency-specific administrative matters;
- Division and group-level procedures; and
- Investigative techniques.

OJT consists of New Employee Orientation and is available on the TIGTA Intranet. The orientation training provides new SAs with fundamental information related to TIGTA's organization, roles, and responsibilities; it also provides an overview of TIGTA-wide policies, procedures, and programs. See Chapter 600, Section 70.26 of the TIGTA Operations Manual for additional information related to new employee orientation not specific to OI.

OJT is designed to give one-on-one instruction and evaluation to new SAs. The trainees will be evaluated on 18 performance tasks by an OJI. New SAs may begin and even complete all 18-performance tasks after entry on duty; however, may not formally graduate from OJT until completion of SABT.

100.5.1 On-the-Job Training Program Completion. The OJT program will be completed no later than 36 weeks after graduation from SABT. After completion of CITP, SABT, and receiving an acceptable rating for all 18 performance tasks, trainees will be eligible to graduate from the program.

100.5.3 On-the-Job Training Program Responsibilities. There are five members of the OJT team, each having distinct responsibilities.

100.5.3.1 Assistant Special Agent in Charge-Training Team. The ASAC-Training Team provides functional oversight for the OJT program, ensuring that the program is effectively implemented and that program objectives are being met at the divisional level.

100.5.3.2 Special Agent in Charge/Director. The trainee's SAC/Director monitors his/her progress toward completion of all OJT program objectives, to include any divisional training requirements.

100.5.3.3 Assistant Special Agent in Charge/Assistant Director. The trainee's ASAC/Assistant Director (AD) routinely meets with the trainee and OJI to establish training priorities and to monitor progress toward the completion of program objectives.

100.5.3.4 On-the-Job Instructor. Each OJI instructs, guides, and mentors the trainee on matters outlined in the OJT manual and provides feedback to both the trainee and ASAC regarding progress within the program.

100.5.3.5 Trainee. The trainee must become thoroughly familiar with the requirements and responsibilities set forth in the OJT manual and must remain open to

feedback, constructive criticism, and suggestions for improvement from the ASAC and OJI(s).

100.6 Firearms, Agent Safety, and Tactics Training.
The Academy develops and oversees firearms, SA safety, and control tactics training. See Section 130.

100.7 Advanced Training.
SAs participate in various training programs to enhance their individual skills and competencies. Advanced training focuses on subject areas such as interviewing; evidence gathering and processing; advanced investigative techniques; firearms and control tactics; leadership; management; and other specialized topics.

TIGTA, IRS, FLETC, CIGIE, and other Federal organizations offer advanced training programs. Detailed descriptions and curriculum outlines for many of these courses are available from the ASAC-Training Team. Attendance in advanced programs is based on mission needs, funding, and availability.

100.8 External Training.
External training is used to satisfy a training need that cannot be met within the training programs offered by TIGTA, IRS, CIGIE or FLETC. This includes training offered by other Government agencies and private vendors. External training requests must meet the following criteria:

- The training is job-related and enhances the attendee's job performance;
- Comparable training is not available within TIGTA, IRS, CIGIE or FLETC, or is too costly and time-consuming to develop;
- The training meets the needs of the organization;
- The sole purpose of the training is not for obtaining a degree; and
- Funding is available.

Information regarding training requests is provided in Section 100.13.

100.9 Continuing Professional Education.
OI endeavors to provide continuing professional education (CPE) annually, based upon availability of funds. The goal of CPE is to provide OI personnel with relevant training to assist them with their professional careers. The training agenda for each CPE changes based on the needs of the organization.

100.10 Leadership Development Program.
The Leadership Development Program (LDP) is a voluntary program for all OI personnel interested in leadership and fulfilling leadership roles. The goals of the program are to promote individual professional development, develop candidates for future leadership positions, assist OI in organization succession planning, facilitate the

transfer of organizational and cultural knowledge, and aid in staff retention.

Management vacancies are filled through the competitive process. All interested personnel should apply for management vacancies as they occur. Participation in the LDP does not guarantee selection, but rather it is one of the resources provided by OI for employees to develop, expand, and refine their leadership and managerial skills.

100.10.1 Leadership Development Program Cadre. The LDP has two cadre levels. The first is designed to identify working-level employees with a desire to become first-line supervisors or leaders. The second cadre is for existing first-line supervisors who have a desire to become senior-level managers or leaders.

OI employees interested in leadership positions are encouraged to continually discuss their career goals with their immediate supervisor. Announcements for the LDP cadre are as-needed.

100.11 Instructor Cadre Program.
The Instructor Cadre Program (ICP) is designed to identify, train, and equip SAs and ASACs who have a desire to become instructors in the OI training program. The goal of the ICP is to have qualified instructors within OI available to assist the Academy in the delivery of agency training programs. As an accredited training academy, all instructors must possess the appropriate certification.

SAs and ASACs interested in participating in the ICP are encouraged to continually discuss their career goals with their immediate supervisor. OI will solicit interested candidates for the ICP as-needed.

100.12 Self-Development Activities.
Self-development activities can improve an employee's job skills and/or provide skills needed for future career goals. Self-development activities include:

- In-service or external training courses;
- Web-based learning offered through the ITMS Skillsoft Library;
- Correspondence courses;
- Temporary assignments to other offices, functions, or agencies;
- College courses; and
- Professional books or journals to include web-based books and references from books 24x7 offered through ITMS.

OI managers should support and encourage the pursuit of self-development activities and assignments. Employees are encouraged to utilize an individual development plan (IDP) to manage and track self-development activities.

100.13 Individual Development Plan.

The IDP is a career plan for acquiring job-related skills and developing specific competencies needed to advance toward career goals. While IDPs are not mandatory, employees are encouraged to keep current IDPs on file and to discuss their goals with their manager. Managers should discuss with employees whether their goals are realistic, attainable, and compatible with organizational goals. If appropriate, managers should offer suggestions of additional or alternative approaches to meeting the employee's goals and help develop a plan to enhance areas needing improvement.

To learn more about IDPs, visit the Office of Personnel Management's website.

100.13.1 Plan Approval. IDPs are approved by the employees' first-line supervisor.

100.13.2 Plan Update. IDPs should be reviewed periodically and updated to reflect any work environment or career goal changes. See Chapter 600, Section 70.19 of the TIGTA Operations Manual for additional information related to IDPs.

100.14 Career Development Program.
The career development program (CDP) is a resource for all OI personnel to enhance personal and professional development. The CDP is administered by the Training Team.

100.15 Training Requests.
OI utilizes two distinct processes for requesting training: in-service training and external training.

100.15.1 In-service Training Requests. Training provided by TIGTA, IRS, and FLETC is "in-service" training. Training at these facilities require the concurrence of the individual's first-line supervisor, approval from the second-line supervisor, and final approval from their respective executive. Training seats in FLETC programs are filled via a waitlist process. For an employee to be placed on a waitlist, the respective first-line supervisor must initiate the Training Waitlist Request Form and route through their management chain for approval and submission to the Training Team.

Upon approval, the Training Team will track in-service training to maintain an accurate individual training record for the attendee.

100.15.2 External Training Requests. Employees who want to attend external training must complete a Standard Form (SF) 182, *Request, Authorization, Agreement and Certification of Training,* using the "external training" option in ITMS and submit it to his/her first-line and second-line supervisors for approval. ITMS requires four levels of approvals for an external training request:

1. First-line supervisor;
2. Second-line supervisor;

3. ASAC-Training Team; and
4. Office manager or purchase cardholder (payer for training).

Additional information related to TIGTA training not specific to OI is contained in Chapter 600, Section 70.19 of the TIGTA Operations Manual.

100.16 Instructor Details to the Federal Law Enforcement Training Centers. TIGTA participates in providing instructional support to the FLETC, either through funding or through detailing TIGTA personnel as instructors. FLETC is located in Glynco, Georgia, with satellite training facilities in Artesia, New Mexico, Charleston, South Carolina, and Cheltenham, Maryland maintains a staff of permanent instructors and agency-detailed personnel. Details to FLETC as instructors are for three-year periods, with an optional one-year extension. FLETC, OI management, and the detailed SA all must agree to the extension.

100.16.1 Recruitment of Agents for Instructor Details. Recruitment is at the GS-13 level. OI management, with the approval of the Director-FLETC, selects SAs. SAs detailed to the FLETC remain employed by OI but are under the daily operational supervision of the FLETC. Individuals selected for this position are generally the first TIGTA SAs encountered by students of other Federal law enforcement agencies who train at the FLETC. For this reason, the highest possible standards must be maintained for this position.

100.16.2 Detail Termination Reassignment Commitment. At the end of the detail to the FLETC, SAs may be reassigned, pending availability, to:

- Their original post of duty at current grade or with pay retention;
- A headquarters function at current grade; or
- Other assignment available upon the mutual agreement of the SA and OI management.

100.16.3 Memorandum of Commitment. SAs selected for this detail receive a memorandum of commitment from their respective executive outlining their reassignment options.

DATE: July 1, 2020

CHAPTER 400 - INVESTIGATIONS

(400)-110 Government Vehicles

110.1 Overview.
This Section establishes Office of Investigations (OI) policy and responsibilities for the use of Government-owned vehicles (GOVs) and Home-to-Work transportation (HTW), and includes:

- Government Vehicles
- Official Use of Government-Owned Vehicles
- Operation of GOVs
- Responsibilities and Oversight
- Types of GOVs
- Vehicle Acquisition and Registration
- Vehicle Emergency Warning Devices
- Home-to-Work and Work-to-Home Use
- Emergency Driving
- Vehicle Parking and Security
- Vehicle Inspection and Maintenance
- Vehicle Expenses
- Vehicle Maintenance and Repairs
- Vehicle Use Reports
- Accidents, Incidents, and Damage
- Excessing GOVs

110.1.1 Acronyms Table.

110.2 Government Vehicles.
GOVs include TIGTA-owned vehicles and vehicles leased from the General Services Administration (GSA) by TIGTA.

110.3 Official Use of Government-Owned Vehicles.
GOVs are for official use only. The use of GOVs is regulated by 31 U.S.C. § 1344. Approved uses of GOVs are detailed in the following:

- 41 CFR § 101-6.4
- Treasury Directive 74-06 and Treasury Directive 74-01
- 31 U.S.C. § 1344
- 26 U.S.C. §§ 61 and 132(f)
- 26 CFR § 1.61-21
- 26 CFR § 1.132-5

110.3.1 Prohibited Use. The use of GOVs for non-official business is prohibited and will result in disciplinary action.

110.3.2 Prohibited Personnel in GOVs. Employees may not transport dependents or other unofficial personnel in GOVs. These passengers are generally limited to:

- TIGTA employees;
- IRS employees;
- TIGTA or IRS employees and family members who are the subjects of protection details;
- Federal, State and local officials; and
- Persons providing official assistance.

110.3.3 Penalties for Misuse. In accordance with 31 U.S.C. § 1349, any employee who willfully misuses a GOV will be suspended for a minimum of 30 days and may be removed from service.

The negligent use or operation of, or damage to, a GOV by an employee may result in disciplinary action. Any misuse that does not rise to a violation of 31 U.S.C. § 1349 will result in other disciplinary action. See Chapter 600, Section 70.8, Employee Relations, and Exhibit (600)-70.3, Table of Offenses and Penalties for additional information.

110.3.4 Parking and Moving Violations. Except in rare circumstances, appropriations law prohibits TIGTA from paying or reimbursing employees for traffic violations, both parking and moving violations. If the violation occurred as a necessary part of an official investigation, payment or reimbursement may be permissible. For authorization to reimburse an employee for traffic violations, the employee's Special Agent in Charge (SAC) must submit a memorandum to the Deputy Inspector General for Investigations, (DIGI) through the appropriate Assistant Inspector General for Investigations (AIGI), explaining why the violation was vital to the conduct of the official investigation. The DIGI's written approval and ticket payment receipt will be attached to the travel voucher.

110.3.5 Alcohol Policy. Do not consume alcoholic beverages or other intoxicants and operate any GOV. Employees who have consumed alcohol while in an off-duty status may not operate the GOV until such time that the employee is no longer under the influence of alcohol and is able to safely operate the GOV.

110.3.6 Utilizing a GOV to Travel to the Federal Law Enforcement Training Center. GOVs may be utilized for official travel to the Federal Law Enforcement Training Center (FLETC), provided the use of the GOV is the most cost effective method of transportation and the trip to and from FLETC will not extend beyond one day of travel. Prior to using a GOV for this purpose in lieu of other transportation modes, a cost comparison must be completed by the traveler. To obtain the mileage rate for your

assigned GOV for use in the cost comparison, contact the Technical and Firearms Support Division (TFSD) via e-mail *TIGTA Inv TFSD for assistance.

110.3.7 Use of Loaner Vehicles during GOV Maintenance/Repairs. The use of a loaner vehicle provided by a maintenance/repair facility while a GOV is at the facility for maintenance/repairs is prohibited.

The Federal Government does not purchase automobile insurance to cover its leased or owned vehicles but rather, it self-insures its own risk of loss. If an employee were to accept a loaner vehicle from the dealership, since the vehicle is not leased or rented by the Federal Government, then use of the loaner vehicle would not be covered by the Government's self-insurance. If something were to happen because of the acceptance of a loaner vehicle, the employee would be personally responsible for all damages if there were an incident or accident. GSA does not authorize the payment of fuel for a loaner vehicle for those same reasons. The fleet card can only be used to pay for fuel expenses for the GOV it is assigned.

110.4 Operation of GOVs.
An OI employee must possess a valid driver's license and have authorization from management prior to using a GOV.

110.5 Responsibilities and Oversight.
TFSD provides oversight of TIGTA's fleet program. The Department of the Treasury provides oversight of all Treasury bureaus' fleet programs. All OI employees are responsible for adhering to the policy as set forth in this Section.

All damage to a GOV regardless of how it occurs must be reported to TFSD and the TIGTA Board of Survey (BOS). See Chapter 600, Section 130.1.

110.5.1 Employee Responsibilities. Before using a GOV, each OI employee must complete Treasury-mandated training regarding vehicle use in the Integrated Talent Management System (ITMS). Each employee is responsible for knowing and complying with all Federal rules and regulations, Treasury and TIGTA policies, and all State and local motor vehicle laws, including but not limited to the following:

- 41 CFR Parts 102-34;
- 5 CFR Part 930, Subpart A;
- Treasury Directive 74-01, *Motor Vehicle Fleet Management*; and
- Treasury Directive 74-06, *Home to Work Transportation Controls*.

Title 41, CFR § 101-39.300 prohibits the use of tobacco products in all GSA fleet vehicles.

Title 41, CFR § 102–34.260 requires the use of safety belts in all Government-owned and Government-leased vehicles.

Each employee who is authorized HTW transportation will:

- Accurately document HTW and Work-to-Home (WTH) usage, fuel purchases, maintenance, call-outs, and mileage using Personal Property Module (PPM);
- Ensure HTW default mileage is correct in PPM, and promptly notify the divisional vehicle coordinator if HTW mileage has changed;
- Accurately input vehicle mileage at the gas pump when fueling the vehicle;
- Report all accidents, incidents, thefts, break-ins, and damage to the first-line supervisor within 24 hours of the occurrence;
- Report the loss or theft of the GSA Fleet credit card to the divisional vehicle coordinator and first-line supervisor within 24 hours of the loss or theft;
- Purchase alternative fuel, when practical, for alternative fuel vehicles (AFVs) and properly document the fuel type in PPM;
- Ensure the vehicle is periodically cleaned and in working condition;
- Periodically check the vehicle for safety hazards and damage;
- Perform scheduled preventative maintenance as required by GSA;
- Promptly address all vehicle recalls;
- Ensure the vehicle is properly secure and safeguard from vandalism, break-ins, acts of nature, and other damage, when possible;
- Report to his/her first-line supervisor, within 24 hours, any time the employee's driver's license is suspended, revoked, or otherwise restricted;
- Complete a Daily Vehicle Log; and
- Complete a monthly PPM Agent Review Report for his/her assigned vehicle.

110.5.2 Supervisor Responsibilities. Before providing authorization for an OI employee to operate a GOV, the first-line supervisor must ensure that the OI employee:

- Possesses a valid driver's license from where the employee is domiciled in the United States or Puerto Rico, and for the type/class of vehicle the employee is authorized to operate;
- Has completed Treasury-mandated training regarding vehicle use;
- Is instructed that the vehicle under the employee's control must be used only for official business and in conformity with Government-wide, Department of the Treasury and TIGTA policies and regulations; and
- Complies with GSA, Treasury and OI policies.

In addition to the above requirements, if the OI employee is authorized HTW use of a GOV, the first-line supervisor should ensure that the OI employee:

- Completes a Daily Vehicle Log; and

- Completes a monthly PPM Agent Review Report for his/her assigned vehicle.

See Section 20.9 for mandatory driver's license requirement for special agents (SA). The first-line supervisor must review with each OI employee who operates a GOV his or her responsibility to:

- Review the procedures for emergency driving;
- Report all accidents, incidents, thefts, break-ins, and damage to the first-line supervisor within 24 hours of the occurrence;
- Practice the rules of safe driving, including the mandatory use of a seat belt (See Chapter 600, Section 40.5.16);
- Ensure the vehicle is periodically cleaned and in working condition;
- Periodically check the vehicle for safety hazards and damage;
- Follow recommended preventative maintenance procedures; and
- Possess a valid driver's license from where the OI employee is domiciled in the United States or Puerto Rico, and for the type/class of vehicle the OI employee is being authorized to operate.

The first-line supervisor will report all accidents, incidents, thefts, break-ins, and damage to the second-line supervisor within 24 hours of receiving notification of the accident, incident, theft, break-in, or damage.

The first-line supervisor will also report the loss or theft of the GSA Fleet credit card to the second-line supervisor within 24 hours of receiving notification of the loss or theft.

110.5.3 Divisional Oversight. Each Special Agent in Charge (SAC)/Director will designate a vehicle coordinator for the division.

The vehicle coordinator will ensure that the division:

- Maintains accurate vehicle records in PPM;
- Maintains accurate monthly PPM Agent Review Reports;
- Maintains accurate information in GSA Drive-Thru;
- Maintains control over vehicle use, assignments, transfers, and disposals;
- Promptly advises TFSD when vehicles are no longer needed or when additional vehicles are required;
- Follows a preventative maintenance program as established by GSA;
- Ensures all vehicles assigned to their division are in working condition for operational reliability and readiness;
- Makes required administrative reports to TFSD, including the annual certification of vehicles assigned to the division;
- Compiles data for the submission of the required annual certification of the condition of the vehicles; and

- Maintains a separate file for each vehicle.

The SAC/Director will ensure the divisional vehicle coordinator attends all mandatory fleet training.

The SAC/Director or second-line supervisor will report all accidents, incidents, thefts, break-ins, and damage to the respective executive and TFSD (via the *TIGTA Inv TFSD) within 24 hours of receiving notification of the accident, theft, or damage. The executive will report the information to the TIGTA BOS.

110.5.4 TFSD Oversight. TFSD provides oversight of the fleet program by:

- Developing policy regarding the fleet program;
- Ensuring TIGTA meets Federal sustainability mandates;
- Managing the fleet budget and lease;
- Performing a vehicle utilization study each fiscal year and making recommendations to right-size of the fleet;
- Coordinating the lease or purchase of vehicles with GSA;
- Coordinating the disposal, transfer, or resale of vehicles with GSA;
- Providing oversight of administrative reporting; and
- Receiving and maintaining copies of accident reports.

110.6 Types of Government-Owned Vehicles.
OI's fleet consists of enforcement vehicles, surveillance vehicles, and pool vehicles.

110.6.1 Enforcement Vehicles. Enforcement vehicles are equipped with emergency warning devices and mobile radios. Installation of emergency warning devices must meet State requirements for identifying law enforcement vehicles. See Section 110.8.

110.6.2 Surveillance Vehicles. Surveillance vehicles are permanently fitted with electronic equipment used for gathering evidence during investigations. Divisional Technical Agents (DTAs) are responsible for the maintenance and readiness of surveillance vehicles. Surveillance vehicles are not authorized for continuous HTW/WTH use and may not be assigned to OI employees in lieu of a standard enforcement vehicle.

When not in use, surveillance vehicles:

- Must be maintained in a secure storage area or facility; and
- Should have access to a dedicated electrical power source to maintain internal battery systems for operational reliability and readiness.

110.6.3 Pool Vehicles. OI maintains a limited number of pool vehicles. Pool vehicles will be assigned to an individual who is responsible for completing the monthly vehicle report and ensuring the vehicle remains operational.

110.7 Vehicle Allocation, Acquisition and Disposal.
OI establishes the number of enforcement vehicles in its fleet based on need and the number of approved HTW positions as determined by the Department of the Treasury.

110.7.1 Vehicle Acquisition and Delivery. OI leases its enforcement vehicles and pool vehicles from GSA. GSA notifies the division's vehicle coordinator when a vehicle is available for pick-up. The division must take delivery of the vehicle within eight days otherwise storage fees may be assessed.

The division must ensure that the new vehicle received is the correct vehicle that was ordered for the division. The driver picking up the vehicle will ensure that the year, make, model, color, and vehicle identification number of the new vehicle matches the information provided by GSA. If there is a discrepancy, do not take delivery and notify the divisional vehicle coordinator who will contact GSA to resolve the issue.

110.7.2 Vehicle Registration. The registration of GSA-leased vehicles varies from State to State. The divisional vehicle coordinator should contact his or her GSA Fleet Service Representative (FSR) for instructions.

110.7.3 Excessing GOVs. TIGTA-owned and leased vehicles are eligible to be excessed or returned to GSA when the vehicle has met the minimum standards for replacement.

When returning a leased vehicle to GSA, the vehicle must be clean and in working condition. Any recalls must be addressed prior to returning the vehicle. All vehicles must be returned with two sets of ignition keys and GSA tags, unless the GSA tags were previously returned to GSA.

See Chapter 600, Section 50.12.8 regarding the disposal of capitalized assets. See Chapter 600, Section 50.12.7.1.1 regarding the restrictions on use of funds received related to GOVs.

110.8 Vehicle Emergency Warning Devices and Mobile Radios.
TFSD purchases all mobile radios, sirens, and emergency warning lights, and approves the installation and removal of equipment in OI's enforcement vehicles. Contact the TFSD Radio Communications Program Manager for equipment needs.

110.9 Home-to-Work and Work-to-Home Use.
TIGTA SAs may be authorized HTW and WTH use of GOVs in accordance with 31 U.S.C. § 1344, Treasury Directive 74-06, and OI HTW determinations.

HTW transportation in a GOV is approved based on the need for the official use of a GOV between the employee's residence and duty station to ensure the safe and efficient performance of intelligence activities, protective services, and law enforcement duties. This includes the need for SAs to be readily available to provide an emergency or investigative response or in support of TIGTA's continuity of operations program. Temporary HTW authorization may be granted based upon the needs of a particular assignment.

110.9.1 Rescinding Home-to-Work Authorization. HTW authorization may be rescinded if the HTW is no longer essential for the safe and efficient performance of intelligence activities, protective services, and/or law enforcement duties.

When an SA is prohibited from carrying a firearm, the SA's authorization for HTW transportation in a GOV will be rescinded because the SA's use of a GOV for HTW transportation is no longer essential to the safe and efficient performance of criminal law enforcement duties, protective operations, and/or criminal intelligence activities.

110.9.2 Training Requirements for Home-to-Work. Employees who have, or are eligible to have, HTW privileges must complete the training courses outlined below in ITMS every fiscal year:

- Defensive Driving Fundamentals;
- IRS Prohibition on Texting While Driving;
- TIGTA OI GSA Fleet Card and Antideficiency Act Training; and
- TIGTA OI Home-to-Work Program.

All OI employees who are authorized to operate GOVs must complete the Defensive Driving and No Texting While Driving modules in ITMS prior to operating a GOV.

110.10 Emergency Driving.
Emergency driving is defined as the use of a law enforcement vehicle by an SA deliberately violating the posted legal speed limit and traffic laws for one or more of the following purposes:

- Following a suspect vehicle to make an apprehension;
- Conducting surveillance; or
- Responding to other exigent circumstances.

Emergency driving is prohibited except when the SA believes that the seriousness of the emergency outweighs the danger created by such driving. SAs will cease emergency driving when it is no longer safe to continue emergency driving.

SAs are responsible for knowing and complying with the appropriate State emergency driving guidelines and requirements applicable to that State's law enforcement officials.

SAs must activate vehicle emergency warning devices, when appropriate, during emergency driving.

110.10.1 Factors to Consider. When balancing the need for emergency driving with safety considerations, SAs should consider all relevant factors, including but not limited to:

- The nature of the emergency;
- The imminent danger to public safety if a suspect is not apprehended;
- The seriousness of the offense;
- The probability of apprehending a suspect at a later time;
- The location, weather, speed, traffic, and road conditions;
- The time of day;
- The presence of pedestrians;
- The officer's driving abilities;
- The condition of all vehicles;
- The availability of emergency equipment;
- The availability of assistance from uniformed police officers in marked police vehicles; and
- The possibility of alternative courses of action.

110.10.2 Decision to Engage/Terminate Emergency Driving. The determination of whether to engage in or terminate emergency driving shall be made by the SA or his/her supervisor in accordance with TIGTA's policy and procedures.

110.10.3 Offensive Tactics. In some circumstances, offensive tactics may constitute the use of deadly force. See Section 120.5 of this chapter for the policy on the Use of Deadly Force.

110.10.4 Felony Vehicle Stop. A felony vehicle stop is an attempt by an SA, in the course of official business, to use a TIGTA law enforcement vehicle to stop a vehicle by using appropriate vehicle emergency warning devices. If the violator disregards attempts to stop him/her and attempts to flee, the SA is prohibited from engaging in emergency driving unless the SA reasonably believes that the failure to engage in emergency driving poses an immediate threat of loss of life or serious bodily injury to the SA or another person.

Intentional contact between a TIGTA law enforcement vehicle and any vehicle attempting to leave the scene and attempts to force the fleeing vehicle off the road are generally prohibited. Such actions are only allowed if the SA reasonably believes that the failure to engage in them poses an immediate threat of loss of life or serious bodily injury to the SA or another person.

110.11 Vehicle Parking and Security.
Employees assigned or using GOVs are expected to exercise reasonable and prudent care as follows:

- Avoid parking in high crime areas when possible;
- Do not leave valuable items in plain view;
- Safeguard the vehicle from vandalism, break-ins, and acts of nature (*e.g.*, hurricanes, floods, tornadoes, hail, etc.) when possible;
- Do not store extra keys to the GOV inside the GOV; and
- Always lock the vehicle doors.

110.12 Vehicle Maintenance and Repairs.
GSA establishes the preventative maintenance program to service vehicles as required. Each division must maintain a record of all maintenance and repairs conducted on vehicles. See FMR 102-34.285 and FMR 102-34.290. The purchase of tires, batteries, and any repairs in excess of $100 requires pre-approval from GSA's Maintenance Control Center (MCC). Any glass repairs must also receive prior approval from GSA's Accident Management Center (AMC). It is the responsibility of the GOV operator to contact GSA's MCC/AMC, as appropriate, for pre-approval.

GOV maintenance and repairs will be paid for with the GSA fleet credit card. The GOV operator is responsible for ensuring that the merchant accepts the fleet card prior to making any purchases. The GOV operator may be personally responsible for payment of any purchases made from a merchant that does not accept the GSA fleet credit card.

110.12.1 Oil Changes. When a GOV is equipped with an oil light sensor (OLS), oil changes must be completed as indicated by the OLS.

If the vehicle is not equipped with an OLS, the GSA FSR will notify the vehicle coordinator to have the oil changed, based on the number of miles driven or time elapsed since the last oil change. The GSA FSR will also notify the vehicle coordinator of any preventative maintenance that should be performed.

Synthetic oil should not be purchased unless the vehicle manufacturer requires it; check the owner's manual for engine oil type.

Unnecessary or unscheduled preventative maintenance (maintenance performed earlier than necessary) is not included in TIGTA's vehicle lease. GOV operators should avoid unnecessary or unscheduled preventative maintenance as it results in additional costs to TIGTA.

110.12.2 Car Washes. There are limits on the number of car washes that may be purchased in a billing cycle. The limits vary and the divisional vehicle coordinator should be consulted for the current allowable amount.

110.12.3 Window Tinting. Window tinting must be paid for using a small purchase card. Purchase requests should be submitted in accordance with your Division's policies and procedures.

110.13 Excessive Wear and Tear.
Excessive wear and tear expenses are not included in the GSA lease and will be billed back to TIGTA as an agency-incurred expense. TIGTA pays for all maintenance-related expenses that GSA determines to be caused by abuse or neglect of the GOV. TFSD reviews all agency-incurred expenses and the GOV operator may be required to prepare a memorandum explaining the excessive wear and tear.

110.14 Manufacturer Recall Notifications.
GSA FSRs serve as GSA's primary interface with vehicle coordinators. GSA FSRs provide notifications to vehicle coordinators when there are open recalls for vehicles within their division. Upon notification from GSA, the vehicle coordinator will notify the GOV operator and his/her supervisor of the recall requirement.

The GOV operator will ensure that the required recall is completed within 45 days of OI's notification of the recall. The GOV operator will notify their vehicle coordinator when the recall has been completed. The vehicle coordinator will clear the recall in GSA Drive Thru within five business days. GSA may remove the GOV from service if a recall is not completed.

110.15 Vehicle Use Reports and Daily Vehicle Logs.
Treasury Directive 74-06 and FMR 102-5 require the reporting of HTW, WTH and after-hours usage. Fuel, maintenance costs, and repairs must be separated and properly identified on the monthly PPM Agent Review Report to meet Treasury and GSA reporting requirements. A daily vehicle log must be maintained for each GOV, including pool vehicles.

The following information must be entered in PPM monthly for each GOV:

- Name and title of operator;
- GOV's identification;
- Dates of use;
- Purpose of the use (*e.g.,* field mileage, training mileage, or maintenance mileage);
- Fuel type purchased;
- HTW and WTH usage; and
- Call-outs.

A call-out is defined as any use of the GOV that occurs outside of the SA's normally scheduled tour of duty, begins or ends at a location other than the SA's post of duty, and is in response to an emergency or an investigation.

110.16 Accidents, Incidents, and Damage.
GSA Fleet defines an "accident" as:

- A crash involving a GSA Fleet vehicle and at least one other vehicle;
- A single vehicle crash that involves a fatality or personal injury to the driver, a passenger, or an individual not located in the vehicle; or
- A crash that involves damage to property.

GSA Fleet defines an "incident" as:

- A single vehicle crash with no fatality, injury, or property damage;
- Vandalism;
- Theft;
- Act of nature; or
- Damage for which the cause is unknown.

FMR 102-34.300, Reporting Motor Vehicle Accidents, requires that each vehicle contain a supply of the following standard forms (SF) for completion in case of an accident:

- SF-91, *Motor Vehicle Accident Report*
- SF-94, *Statement of Witness*

Any GOV operator who is involved in an accident and/or an incident may be required to take additional driver training in accordance with Treasury policy.

110.16.1 Accident Response. When a GOV is involved in an accident, the GOV operator should ensure that emergency personnel are contacted, if necessary. The GOV operator will attempt to obtain a SF-94 from all available witnesses and will take photographs of the vehicle and/or property damage. If the accident involves a GOV, the operator will notify the GSA's AMC.

The GOV operator will also ensure that a police report is prepared if the GOV accident involved:

- Physical injury to any person;
- Collision with another motor vehicle;
- Estimated property damage exceeding $250; or
- Damage to the GOV that would impair the vehicle's safe operation.

The police report is an important factor in proving fault. If a police report is prepared, the GOV operator will provide the police report to the AMC.

The GOV operator should obtain the following information at the scene of the accident:

- Name of the other driver(s) involved in the accident, along with his or her phone number and home addresses;
- Insurance information from the other driver(s) to include company name, address, phone number, and policy number; and
- Names and contact information of witnesses, if applicable.

DO NOT sign any documents or make any statements as to who was at fault.

The GOV operator must take photos to document the scene. The photos of the vehicle and the scene should be included with the SF-91. The photos should document:

- Damage to vehicles and/or property;
- Accident/incident scene including road conditions, skid marks, debris in roadway, and vehicle positions;
- Location identifiers of the accident scene such as intersection, address, or exit number; and
- Drivers' and vehicles' identification such as driver's licenses, insurance cards, license plates, etc.

See AMC Customer FAQs regarding GOV accidents.

110.16.1.1 Government-Owned Vehicle at Fault. When a GOV operator damages a third party's vehicle, the operator should advise the third party to contact TIGTA Counsel at (202) 622-4068, who will advise them on how to file a claim.

110.16.1.2 Third Party at Fault. If a GOV is damaged by an identifiable third party, GSA will initiate a claim against the third party to pay for the damages.

110.16.2 Reporting Requirements. The GOV operator must notify his/her first-line supervisor within 24 hours of any GOV accident, incident, theft, or damage (other than normal wear and tear). The first-line supervisor will immediately notify the second-line supervisor of the accident, incident, theft, or damage, and the second-line supervisor will immediately notify their respective executive and TFSD via *TIGTA Inv TFSD.

The second-line supervisor will submit their written notification and supporting documentation to their respective executive, who will submit the information to the BOS Coordinator at *TIGTA BOS, TFSD at *TIGTA Inv TFSD, and TIGTA Office of Chief Counsel at *TIGTA Counsel Office, within 24 hours of receipt of the incident information. See Chapter 600, Section 130.1.

All accidents must be reported to the AMC within five business days.

An incident normally involves damages caused by an object striking the vehicle and causing damage (*e.g.,* rock flying up and hitting the vehicle, something falling onto the vehicle). When a GOV is involved in an incident, the GOV operator is responsible for completing a SF-91, and must type or print the word "INCIDENT" on top of the form. Hail damage and vandalism are considered incidents. Reporting incidents follows the same procedures as accident reporting outlined in this subsection, to include supervisory and BOS procedures. Notifying the AMC is not required for incidents; TIGTA is solely responsible for paying for incident repairs.

See Exhibit (600)-130-2 for a sample BOS memo.

In addition to notifying the first-line supervisor and the AMC, the following reports will be completed, as applicable:

- **Accident Report –** The GOV operator or designated official will complete a thorough SF-91 detailing the pertinent events related to the accident. The accident report should also include police reports, photographs, witness statements (SF-94), hospital reports, towing records, damage estimates, and other relevant information, as appropriate. The first and second-line supervisors are responsible for ensuring that all reports are complete, accurate and timely. The second-line supervisor will forward the original accident report to their respective executive, who will ensure that the approved report is distributed to TFSD, TIGTA Counsel, and the TIGTA BOS.

- **Workers' Compensation Claim –** Report any injuries sustained as a result of a GOV accident to the first-line supervisor and in accordance with the procedures in Chapter 600, Section 90.5 of the TIGTA Operations Manual.

- **TIGTA Injury/Incident Review Report –** If a TIGTA employee sustains an injury in a GOV accident, the first-line supervisor must notify TIGTA OMS of the injury/incident by completing a TIGTA Injury/Incident Review Report. See Chapter 600, Section 90.8 of the TIGTA Operations Manual for TIGTA injury/incident reporting procedures.

- **TIGTA Board of Survey –** The SAC will prepare a memorandum and forward to their respective executive who will provide written notification to the TIGTA BOS of the loss, theft, or damage of any GOV per Chapter 600, Section 130 of the TIGTA Operations Manual.

110.16.3 Accident Repairs. GSA pays for all repairs to GSA-leased vehicles that are required to return the vehicle to a safe and working condition. After the repairs or damages are assessed, GSA bills TIGTA for all repair costs and damages unless an identifiable third party is at fault.

If the GOV operator believes he or she was not at fault, and the GOV operator has the proper documentation of fault (***e.g.***, police reports, admission of fault, etc.), then the AMC will process the claim with the other driver or their insurance company.

The GOV operator must complete Section II of SF-91 in its entirety. Without complete information, the AMC Claims Resolution Section will be unable to process the claim and TIGTA will be responsible for all repair costs associated with the accident.

If the AMC cannot determine that the other party was at fault because of lack of proper documentation or police report determining fault, the AMC will bill TIGTA for the entire repair cost.

DATE: October 1, 2017

CHAPTER 400 – INVESTIGATIONS

(400)-120 Use of Force and Critical Incidents

120.1 Overview.
This section establishes the Office of Investigations (OI) policy and procedures regarding use of force by OI special agents (SA) in pursuit of TIGTA's law enforcement mission. It includes essential information related to the use of force and response to use of force and critical incidents by OI personnel. SAs must be knowledgeable about the policies and procedures contained in this section, which include the following:

- Reporting Requirement
- Use of Force
- Use of Non-Deadly Force
- Use of Deadly Force
- Use of Force Incident
- Unintentional Discharge of a Firearm Response
- Investigation of Use of Force Incident and Unintentional Discharge of a Firearm
- Shooting and Assault Review Committee
- Critical Incident
- Active Threat
- Active Threat Response Plan
- Active Threat Response Training
- Continuity of Operations Program

120.1.1 Acronyms Table.

120.1.2 Definitions.

Deadly Force is the use of any force that is likely to cause death or serious physical injury in pursuit of a law enforcement objective. Deadly force does not include force that is not likely to cause death or serious physical injury, but unexpectedly results in such death or injury.

Non-Deadly Force is the use of a reasonable level of force, other than deadly force, necessary to execute an arrest or otherwise accomplish a law enforcement objective.

A **Shooting** is defined as:

- A discharge of a TIGTA-issued firearm occurring outside of firearms training, regardless whether such discharge was intentional or unintentional or occurred on duty or off duty;

- A discharge of a TIGTA-issued firearm during training that results in death or personal injury;
- An unintentional discharge of a personally-owned firearm that results in death or injury; or,
- Any discharge of a personally-owned firearm during or results in law enforcement intervention.

Use of Force Incident is any use of force in pursuit of a law enforcement objective (*e.g.*, discharge of a TIGTA-issued firearm, use of an intermediate weapon, weaponless control techniques, physical force) by a TIGTA SA or by any officer or agent of another agency during a joint investigation and/or enforcement operation with TIGTA that results in death, injury, or property damage.

120.2 Reporting Requirement.
The following events must be reported to the Assistant Special Agent in Charge (ASAC) or a higher-level manager as soon as possible:

- Any use of force incident (see the use of force incident definition in Section 120.1.2);
- Any shooting incident (see the shooting definition in Section 120.1.2);
- Any use of a TIGTA-issued intermediate force weapon, other than at training events;
- Any discharge of a firearm that causes the SA's position as a Federal law enforcement officer to be made known or impacts the SA's position as a Federal law enforcement officer.

The Special Agent in Charge (SAC) must promptly notify the appropriate Assistant Inspector General for Investigations (AIGI) or Deputy Assistant Inspector General for Investigations (DAIGI), and the SAC, Internal Affairs Division (IAD) by telephone.

120.3 Use of Force.
The Treasury Use of Force Policy is contained in Treasury Order 105-12. The primary consideration in any use of force situation is the timely and effective application of the appropriate level of force required to establish and maintain lawful control. A paramount consideration is the preservation of life and prevention of bodily injury. The use of force is based upon the threats presented and the subject's degree of compliance or noncompliance.

SAs will apply a reasonable level of force necessary to achieve their law enforcement objective based upon their perceptions of the actions of the subject.

120.4 Use of Non-Deadly Force.
SAs will use a reasonable level of force necessary to execute an arrest or otherwise accomplish the law enforcement objective.

120.4.1 Use of Weaponless Control Techniques. When appropriate, SAs will utilize weaponless control techniques, including officer presence, identification, verbal commands, comealongs, touch pressure points, and empty hand strikes.

120.4.2 Use of Intermediate Weapons. When appropriate, SAs will utilize a TIGTA intermediate weapon, including an oleoresin capsicum aerosol and/or an extendable baton. See Section 130.9 for more information on intermediate weapons.

120.5 Use of Deadly Force.
SAs may use deadly force only when necessary in pursuit of a law enforcement objective, that is, when the SA has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the SA or to another person.

120.5.1 Use of Verbal Warnings Prior to Use of Deadly Force. If feasible, and if doing so would not increase the danger to the SA or others, SAs must give a verbal warning to the subject to submit to the SA's authority prior to the use of deadly force.

120.5.2 Use of Deadly Force Against Fleeing Felons. Deadly force may be used to prevent the escape of a fleeing suspect if there is probable cause to believe that:

- The subject has committed a felony involving the infliction or threatened infliction of serious physical injury or death; and,
- The escape of the subject would pose an imminent danger of death or serious physical injury to the SA or other persons.

120.5.3 Use of Deadly Force Involving Moving Vehicles. Weapons may not be fired solely to disable moving vehicles. Weapons may be fired at the driver or other occupant of a moving vehicle only when:

- The SA has a reasonable belief that the subject poses an imminent danger of death or serious physical injury to the SA or other persons; and,
- The public safety benefits of using such force outweigh the risks to the safety of the SA or other persons.

120.5.4 Use of Deadly Force Against Vicious Animals. Deadly force may be directed against dogs or other vicious animals, when necessary, in self-defense or defense of others.

120.5.5 Use of Warning Shots. Warning shots are not permitted.

120.6 Use of Force Incident.
All use of force incidents will be handled as described in this section. See 120.1.2 and 120.2 of this section for use of force incident definition and reporting requirement.

Any TIGTA employee involved in a use of force incident will be placed in administrative duty status and/or may be placed on leave. The SAC, DAIGI or appropriate AIGI, or the Deputy Inspector General for Investigations (DIGI) may grant administrative leave. See Chapter 600, Section 70.4.8 for guidance on granting administrative leave. See Exhibit (400)-120.3 for TIGTA's Use of Force Incident Checklist.

120.6.1 Senior SA Responsibilities. In a use of force incident, the senior SA on the scene, unless otherwise unable, shall assume responsibility for the scene until relieved by an ASAC or other TIGTA OI manager. A senior SA is defined as the highest graded SA on the scene. In the event all of the SAs are the same grade level, the senior SA is considered to be the SA who has seniority at TIGTA. The senior SA on the scene is responsible for coordinating the following:

- Making sure the area is safe;
- Immediately securing medical aid for injured parties. If a person is injured by an SA, make a reasonable effort to provide first aid and to make medical attention available to the person. An SA has no authority to commit Federal funds for payment of medical expenses;
- Notifying the appropriate local law enforcement agency and securing the scene of the incident until their arrival;
- Separating all SAs involved in the incident and/or witnesses, as soon as possible;
- Preserving evidence until it can be collected by local law enforcement or other law enforcement agency having jurisdiction to investigate the matter. Do not collect or move evidence unless absolutely necessary. If evidence must be moved, clearly mark its location and position;
- Identifying individuals with knowledge of the incident for interviews at a later time by local law enforcement and TIGTA SAs;
- Immediately notifying his/her ASAC or SAC, regardless of the time of day;
- Cooperating with the responding law enforcement agency by presenting identification and providing such information as is consistent with official duties of the involved SA (*e.g.*, firearms were discharged while acting in an official capacity, medical assistance has been requested, suspects are in custody);
- Not disclosing confidential information (*e.g.*, grand jury, tax returns and return information) when discussing the incident;
- Not allowing media personnel to interfere with the crime scene or with involved personnel; and,
- Assigning SAs to accompany injured suspects to the hospital to record statements. If possible, these SAs should be agents not involved in the incident.

120.6.2 ASAC Responsibilities. An ASAC will be dispatched to the scene of a use of force incident. If an ASAC or other TIGTA OI manager is not available to respond, then

the senior SA on the scene will assume the role of the ASAC. An ASAC at the scene is responsible for the following:

- Removing the SAs who were involved as primary participants or as witnesses from the scene after advising the investigative agency;
- Assisting the employees involved in the incident, as needed;
- Assigning a companion to assist employees involved in the incident. The companion should be a person not involved in the incident;
- If an SA discharged a firearm that resulted in death, injury, or property damage, taking possession of the firearm and surrendering it to the investigating law enforcement agency with the approval of the SAC, a higher-level OI manager, or their designee. See 120.6.5 for further guidance on disposition of a firearm;
- Inspecting the firearms of all TIGTA SAs at the scene to ensure that all firearms fired and not fired during the incident are identified;
- Ensuring that the involved SA's family is advised that a family member was involved in an incident. If feasible, the contact should be someone who knows the family. If the SA is injured, ensure that the family has transportation to the medical facility. After evaluating the circumstances and on a case-by-case basis, the ASAC can authorize, with the approval of the SAC or higher-level OI manager, an SA to use a Government-owned vehicle to transport the family to the medical facility;
- Remaining at the scene until all physical evidence has been collected, all appropriate investigative details have been attended to and the investigative agency has departed the scene. Where appropriate, the ASAC shall respond to inquiries posed by the investigative law enforcement agency; and,
- Referring all inquiries from the news media to the TIGTA Office of Communications.

120.6.3 SAC Responsibilities. In a use of force incident, the SAC is responsible for the following:

- Immediately dispatching an ASAC and SAs to the scene of the incident to act as liaison and provide investigative and other assistance;
- Immediately notifying the appropriate DAIGI, AIGI or the DIGI by telephone;
- Assigning a TIGTA point of contact to assist the family/survivors when an SA is injured or killed. See the TIGTA OI Survivor Protocol Guide for information on providing assistance to family/survivors of a deceased OI employee;
- Notifying the SAC-IAD of the incident;
- Consulting with the U.S. Attorney's office (USAO) in the SAC's geographical area to discuss the USAO's guidelines and TIGTA's policy on use of force (these discussions should be held prior to an incident);

- Making an initial statement to the media as specified in Exhibit(400)-120.1, only after consultation with TIGTA Counsel and referring all further inquiries of the news media to the TIGTA Office of Communications;
- Briefly advising the division that a use of force incident occurred; and,
- Preparing a Form OI 2020, Fact Sheet, within 24 hours of the incident, unless otherwise directed, that includes the following information in the case synopsis section:

    - A synopsis of the incident, including the case number, if case related;
    - Date, time and place of the incident;
    - Type(s) of firearm(s) and the approximate number of rounds of ammunition fired, if known;
    - If an assault, state the type of weapon used (*e.g.*, gun, bomb, knife, *etc.*);
    - Injuries caused or received;
    - Description of property damage, if applicable;
    - Names of any persons arrested and list of offenses charged;
    - Identification of other persons witnessing or involved in the incident; and,
    - Name and address of any other agency investigating the incident, including agency case number, name and telephone number of the assigned investigator, if known at the time of the notification.

120.6.4 Executive Responsibilities. The DAIGI, appropriate AIGI or the DIGI will advise the TIGTA Office of Communications of possible media contacts and request that the Office of Communications not release the names of involved SAs, IRS employees, or assisting law enforcement officers.

The DAIGI, appropriate AIGI or the DIGI will briefly advise all OI employees that a use of force incident occurred.

120.6.5 Firearms Disposition. A TIGTA SA who discharges a firearm during a TIGTA law enforcement operation may be requested to furnish the TIGTA-issued firearm to the investigating law enforcement agency. If this occurs, a TIGTA SA involved in the incident will not surrender his/her firearm directly to any non-TIGTA investigative agency. The senior TIGTA SA on the scene will advise the investigating law enforcement agency of TIGTA's policy on surrendering a firearm. The SAC or a higher-level TIGTA OI manager must be consulted and approve of the transfer of a TIGTA-issued firearm to a Federal, State or local law enforcement agency.

The SAC or higher-level OI manager should consider the following when determining to surrender a TIGTA-issued firearm:

- Purpose of the surrender (*e.g.*, evidence, ballistic testing);
- Request is reasonable (*e.g.*, needed for the investigation of the incident); and,
- Serial number, make, and model of the TIGTA-issued firearm are documented on a receipt.

If the TIGTA-issued firearm will be surrendered, the firearm will be provided to the ASAC or the senior TIGTA SA on the scene, who will surrender it to the appropriate law enforcement agency. The ASAC or the senior TIGTA SA on the scene will obtain a receipt that contains the serial number, make, and model of the firearm.

A TIGTA-issued firearm that is discharged in a shooting will be taken out of service and its working condition will be examined by the National Firearms, Agent Safety, and Tactics (FAST) Coordinator (NFC), unless the firearm is being held as evidence or for ballistic testing by another law enforcement agency. Once a firearm is returned by another law enforcement agency, forward it to the NFC for examination.

If there is no resulting death, injury, or property damage, the NFC, or a person designated by the NFC, will examine the firearm before it is returned to service.

Based on the circumstances, the SAC will determine if another firearm will be issued to the SA.

120.6.5 Statements and Interviews. Any TIGTA employee involved in a use of force incident, either as a primary participant or witness, may be interviewed by TIGTA and/or any other investigating law enforcement agency. A TIGTA employee has the same constitutional and procedural protections afforded to all subjects of a criminal investigation and/or prosecution (*e.g.*, the right to remain silent, the right to due process, the right to counsel).

Any TIGTA employee involved in a use of force incident will inform the SAC, or his/her designee, before he/she is interviewed as a primary participant and/or witness by any investigating law enforcement agency. A TIGTA employee will not be interviewed until the employee has:

- Been removed from the scene;
- Met with TIGTA management;
- Been afforded a reasonable amount of time, at least 24 hours, to compose himself/herself, consult with legal counsel, and is capable of understanding and exercising his/her rights; and,
- Has a TIGTA management representative with him/her during the interview, if desired by the employee.

An interview should be limited in frequency and conducted only after the investigating law enforcement agency has sufficiently progressed in their investigation to ask all relevant questions in the interview.

All statements made by a TIGTA employee to any TIGTA investigator or to an employee of another law enforcement agency are not privileged or protected. Except as noted below, statements made to Department of Justice (DOJ) attorneys or state prosecutors are not generally covered by the attorney-client privilege.

120.6.6 Requesting DOJ Representation. A TIGTA employee may request DOJ representation in civil actions and in state criminal proceedings arising from his/her employment, including use of force incidents. DOJ representation is generally not available in Federal criminal proceedings.

Official requests for DOJ representation must be made by the TIGTA employee, through the SAC, to TIGTA Counsel. While communications between a TIGTA employee and TIGTA Counsel attorneys during the inquiry process to determine eligibility for DOJ representation are considered privileged communications, communications to the employee's management are not. As such, the request for DOJ representation should state the matter or incident for which representation is requested and should avoid specific details related to the facts or circumstances involved. After the inquiry phase is completed, and if DOJ decides not to represent the TIGTA employee, any further communication with any of these attorneys, is not privileged. See Chapter 700, Chief Counsel, Section 80.1 of the TIGTA Operations Manual for further guidance on DOJ representation.

120.6.7 Employee Assistance. A TIGTA employee involved in a use of force incident that results in death or serious injury must attend a counseling session provided by an IRS Employee Assistance Program (EAP) counselor or other designated counselor, as soon as practical after the incident. TIGTA OI managers should be cognizant that other persons, such as office support staff and family members, may also experience trauma after a use of force incident. IRS EAP is available to all TIGTA employees and their families.

Statements made to EAP or other counselors are generally privileged from access and disclosure in civil litigation. Such statements may not be considered privileged in Federal or state criminal proceedings.

120.7 Unintentional Discharge of a Firearm Response.
Following consultation with an AIGI or DAIGI, the NFC in conjunction with the appropriate Divisional FAST Coordinator (DFC), will arrange for remedial training for the TIGTA SA who unintentionally discharges a TIGTA-issued firearm.

120.8 Investigation of Use of Force Incident and Unintentional Discharge of a Firearm. Multiple agencies may be involved in use of force investigations, including local law enforcement agencies and the Federal Bureau of Investigation. Generally, the primary purpose of any TIGTA investigation will be to investigate potential issues involving the TIGTA SA's actions.

120.8.1 Roles and Responsibilities. The SAC-IAD will determine if an investigation of a TIGTA use of force incident or unintentional discharge of a firearm is warranted. IAD is responsible for conducting all investigations into TIGTA use of force incidents and unintentional discharges of a firearm; however, the SAC-IAD, with the concurrence of an AIGI, may refer an investigation that does not involve the discharge of a firearm to a field division.

If the investigation is referred to a field division, the investigation must be conducted by an ASAC from a division that was not involved in the incident. The appropriate AIGI will select the ASAC who will conduct the investigation. The SAC-IAD will monitor the progress of the field division's investigation. Upon receiving the assignment, the ASAC must immediately contact the SAC-IAD.

120.8.2 Investigation Requirements. TIGTA's investigation will include, but will not be limited to, the determination of facts directly related to the use of force incident or unintentional discharge of the firearm. All TIGTA employees and others that have direct knowledge of the incident will be interviewed. Events and circumstances leading to the incident, such as training, equipment, investigative issues, raid planning, *etc.*, will also be reviewed. The investigating agent or ASAC will immediately advise the SAC-IAD of any indications of individual culpability or continuing safety problems for appropriate action.

The investigating agent or ASAC will prepare a Form OI 2028, *Report of Investigation* (ROI), narrating the results of the investigation. The ROI will be provided to the SAC-IAD as soon as possible, but no later than 30 days after the incident, unless otherwise directed by the SAC-IAD. The ROI will include the following:

- A brief synopsis of the underlying investigation, including the type of investigation, if appropriate, and an overview of the incident; and
- A chronology of events, including, but not limited to, the following areas, as applicable:
  - Events and circumstances occurring prior to the incident, including any raid/arrest briefings;
  - Identification, assignment, and location of all persons present during the incident including TIGTA personnel, other law enforcement personnel, witnesses, and suspects;
  - Suspect's identification, including name, date of birth, address, criminal record, pending criminal charges, and current status;

- Information concerning the suspect's/victim's actions and statements before, during and after the incident, including any evidence of drug or alcohol use, belligerence, or threatening behavior with or without a weapon;
- Description and identification of all discharged firearms, expended ammunition, the identity of the possessor of each discharged firearm at the time of the incident;
- Description of any verbal warnings given to the suspect. If no verbal warning was given, the basis for such decision;
- An accounting of all rounds of ammunition fired;
- Information regarding the manufacturer and/or source of acquisition of any discharged TIGTA firearms;
- Results, when available, of technical examination of TIGTA firearms by an authorized person, relative to operation of the weapon;
- The basis for the decision to use deadly force or other force resulting in death or injury;
- Identification of all injured persons, including cause and extent of injuries, and medical treatment provided;
- Identification and value of any property damage, including cause, extent of damage, and responsible party;
- The date and time of notification to the ASAC or SAC;
- Any unique factors contributing to the incident (*e.g.*, weather conditions, equipment, communications, misinformation, operational planning, *etc.*);
- Topics or issues that should be reviewed by the Shooting and Assault Review Committee (SARC); and,
- List of exhibits and the following exhibit items, as available:
    - Copies of any statements and/or reports of interview provided to other law enforcement agencies;
    - Copies of all operational plans;
    - Copies of all official reports from other investigative agencies;
    - Schematic drawing of the shooting scene;
    - Photographs;
    - List of all relevant evidence recovered at the scene of the incident;
    - Copies of any arrest/search warrants;
    - The TIGTA SA's firearm qualification records;
    - Documentation of method of acquisition of involved firearms;
    - Press releases and/or newspaper reports to determine amount and type of media coverage; and,
    - Any other relevant items.

The final ROI will be provided to the SAC-IAD. Upon review of the ROI, the SAC-IAD may mandate additional inquiries.

120.9 Shooting and Assault Review Committee.
All TIGTA use of force incidents and unintentional discharges of a firearm that are investigated will be reviewed by the SARC. The SARC will normally be convened within 30 days after the submission of the ROI.

The SARC is comprised of the following persons:

- AIGI-Threat, Agent Safety and Sensitive Investigations Directorate;
- SAC-IAD;
- SAC-Operations;
- TIGTA Counsel;
- SAC-Technical and Firearms Support Division; and
- Two senior level managers from other Federal law enforcement agencies.

The SAC-IAD serves as the chairperson. The SARC will review each incident to determine the following:

- If the facts and circumstances surrounding each event have been accurately and completely reported;
- If the TIGTA employee was acting within the scope of his/her authority;
- If the employee's actions were reasonable, legal, and within policy; and
- If the use of force was justified.

If the SARC finds all of the above to be true, the SARC can administratively close the investigation. If the SARC determines there was misconduct or malfeasance by a TIGTA employee, the findings will be provided to the appropriate management official for administrative adjudication. The SARC will also make recommendations, where appropriate, relating to training, equipment, procedures, *etc.*

The SAC-IAD will brief the OI Executive Leadership Team on the findings of the SARC.

The Deputy Special Agent in Charge- Investigative Support and the ASAC-Training Team will review the incident to revise training curricula and incorporate "lessons learned," as warranted.

120.10 Critical Incident.
For the purposes of this section, a critical incident is an unforeseen event that seriously impacts IRS or TIGTA personnel and/or facilities by causing serious injury or loss of life, significant property damage, threat to service/operations, and/or partial or complete disruption of Federal tax administration.

Note: If field division personnel are attending an off-site meeting or conference, the meeting location, date(s), and other pertinent details must be communicated to the Criminal Intelligence and Counterterrorism Division (CICD) in advance.

120.10.1 Critical Incident Response. Except for active threat response situations, SAs are not trained to identify, assess, or directly respond to critical incidents. However, the SA may be a "first responder" to a suspected critical incident. The types of critical incidents that a TIGTA SA may respond to include the following:

- Hazardous material;
- Chemical, biological, radiological, nuclear, and explosives;
- Active threat response situation;
- Hostage situation;
- Barricade situation;
- Sudden severe weather (*e.g.*, ice, tornado);
- Loss of utilities (*e.g.*, blackout);
- Physical attack; and
- Terrorist event.

120.10.2 Response Considerations. When responding to a suspected critical incident, the SA should treat the incident as a crime scene. Other than an active threat response situation and, depending on the circumstances of the critical incident, the SA should respond as follows:

- Remain calm;
- Assess the situation before taking any action;
- Do not attempt to touch, smell, taste, or remove potentially contaminated material;
- Remove ambulatory victims from the hazard area;
- Ensure the area is cleared of personnel and maintain a safe distance;
- Contact the appropriate law enforcement agency and/or response unit;
- Ensure the safety of other responders;
- Represent TIGTA's law enforcement interest in the incident; and
- Establish contact with the senior IRS official on site, if the incident involves an IRS facility.

See Section 120.11 for active threat response.

Note: SAs should cooperate with the law enforcement agency and/or response unit having jurisdiction to investigate the incident.

SAs should try to avoid:

- Entering scene unless absolutely necessary;
- Allowing any unnecessary access;
- Touching or moving anything unless absolutely necessary;
- Conducting an independent search for evidence;
- Taking an agent's firearm unless directed to by investigative authority;
- Releasing any information;
- Leaving the scene until properly relieved; and
- Conducting independent, post-scene investigations.

120.10.3 Initial Assessment. The initial assessment and the circumstances surrounding the incident or event will dictate the agency response (*e.g.*, loss of life, powdery substance incident, IRS employees forced to evacuate, *etc.*). See Section 120.11 for responding to an active threat response situation. SAs are expected to make an initial assessment of the critical incident to obtain information and communicate that information to field division management. Questions to think about at the scene of the incident to convey important information to management may be as follows:

- Who was involved in the incident?
- What actually happened?
- When did the incident take place?
- Where did the incident happen (location)?
- Why did the incident take place?
- Are any people hurt?
- How many individuals need assistance?
- Is this incident an ongoing event?
- Has a local, State, or Federal agency and/or response unit with investigative jurisdiction arrived on the scene?

120.10.4 Notification by Divisions. SAs who respond to a critical incident will, except in an active threat response situation, immediately notify their immediate supervisor or higher-level manager of the incident and any pertinent information related to that critical incident. The SAC-Division will immediately notify the OI Executive Leadership Team of the incident. The DAIGI/AIGI will ensure that the CCID has been notified and respond to the division regarding the decision to activate the Headquarters Command Center, as appropriate.

The SAC-Division will deploy any TIGTA SA who is available, reaching out to agents responsible for the post of duty or the nearest agent who can also provide immediate response. The SAC-Division may also reach out to IRS Criminal Investigation if needed for assistance.

The SAC-Division will coordinate the interdivisional allocation of resources with the DAIGI/appropriate AIGI as well as interagency resources, if required.

SAs will contact the agency or department that has control over the scene to obtain information on the critical incident and communicate that information to their immediate supervisor or higher-level manager who will advise CICD.

120.10.4.1 Notification in Active Threat Response Situations. In an active threat response situation, SAs who respond will notify their immediate supervisor or higher-level manager once the situation is contained and time allows.

120.10.4.2 Command Center. If the Headquarters Command Center is activated, the command center will be located at 1401 H Street, NW, Washington, DC 20005.

120.10.5 CICD Responsibilities. CICD will be the primary point of contact for all critical incidents. During a critical incident, CICD will man the command center at OI Headquarters. CICD will control information that comes into or is disseminated from Headquarters and will validate the veracity of the information. CICD will display the critical incident information for review by the OI executives in the command center.

OI executives will oversee the coordination of the information. OI executives will assess the situation and make a determination as to whether any additional resources (SAs, ASACs or SACs) are needed to maintain daily business operations in the division(s).

120.10.5.1 Notifications from CICD. CICD receives information through classified and unclassified sources. The SAC-CICD will notify the OI executives regarding the incoming information.

The CICD staff will facilitate the transfer of accurate and consistent information to the OI executive team. All requests for information and/or assistance from CICD will be made through the respective division SACs.

120.10.6 Communication. OI executives will ensure the coordination of information between TIGTA, the IRS, and the Department of the Treasury as needed. In addition, the SAC-Division must continuously update CICD with emerging information about the critical incident to ensure OI executives are advised of any status changes.

The SAC-Division is responsible for ensuring that accurate and timely information is provided to OI Headquarters, including whether or not the division is experiencing any communication problems (*i.e.*, email or text communication may work but cell phone coverage may not work, *etc.*).

CICD will utilize the Threat Information Notification System (TINS) format to communicate critical incident information to OI managers and executives. This format

provides information such as a description of the critical incident, the location, the identity of the subject(s), and may request a reply from the division regarding any assets that can be deployed. See Section 410.18 for TINS information.

120.10.7 Media Coverage. OI executives will coordinate all media communications with the TIGTA Office of Communications. SAs will not answer questions asked by any media personnel. SAs will refer any questions from the media to the SAC-Division or the TIGTA Office of Communications.

120.10.8 Impacted Individuals. Employees who are involved in the response to a critical incident, and employees who are victims of the critical incident will participate in EAP, as necessary. The SAC-Division, to the extent possible, will communicate pertinent information regarding the critical incident to impacted parties as the situation dictates. The SAC-Division will also ensure that follow-up communications are conducted with the impacted parties after the critical incident is contained.

120.11 Active Threat.
The term "active threat" refers to an individual or individuals who are causing or threatening to cause death or serious bodily injury to others, usually in a populated area. For the purposes of this policy, "active threat" includes active shooters. Active threat response situations are unpredictable, evolve quickly, and must be assessed on a case-by-case basis, as individual circumstances will dictate the type of response. Special agents must adapt their response to an active threat response situation based upon their training.

120.11.1 Preparing for an Active Threat Response Situation. To be prepared for an active threat response situation, SAs are required to carry their TIGTA-issued handgun and related equipment during core business hours and while on duty (if outside core business hours) unless they are acting in an undercover capacity, are prohibited by policy from doing so, or when judgment or policy dictates that non-carry is appropriate (*e.g.*, Federal courthouse, prison, or similar facility restricting the carry of firearms). During active threat response situations, SAs are authorized to immediately deploy shotguns and rifles without prior supervisory approval.

120.11.2 Active Threat Response. In the event of an active threat response situation involving potential injury or death to IRS employees, TIGTA employees or others, SAs in the immediate area are authorized to immediately respond. SAs may engage and neutralize the active threat consistent with active threat response training.

Armed TIGTA personnel will coordinate their response with other on-scene law enforcement personnel to eliminate the active threat.

120.11.2.1 Notification to Local Law Enforcement. As soon as practical, TIGTA personnel will notify local law enforcement of the situation. Be prepared to describe the known circumstances of the incident such as:

- Location of TIGTA SAs on scene;
- Number of TIGTA SAs on scene;
- Physical description of TIGTA SAs on scene;
- Location of subject(s);
- Number of subjects;
- Physical description of subject(s);
- Number and type of weapon(s) held by subject(s);
- Number of potential victims at the location;
- Any other pertinent information.

120.12 Active Threat Response Plan.
Each SAC shall develop an Active Threat Response (ATR) plan for addressing and responding to an active threat response situation occurring in an IRS office co-located with TIGTA as well as any TIGTA post of duty located within their area of responsibility. The plans will vary due to the size and location of each office.

The ATR plan is a framework of how to respond to an active threat at the given site. The ATR plan should be a coordinated plan in which armed TIGTA personnel work jointly with other Federal, State and local law enforcement personnel for the given area. Outreach to other agencies to discuss their response to TIGTA and/or an IRS workspace in the event of an active threat is critical. The SAC will review the ATR plan annually and update as necessary. See Exhibit (400)-120.2.

120.13 Active Threat Response Training.
The training for active threat response situations will be provided through the TIGTA FAST Program; the TIGTA OI Training Academy; and/or the Federal Law Enforcement Training Center.

120.14 Continuity of Operations Program.
CICD is responsible for the TIGTA Continuity of Operations Program (COOP). The SAC-CICD or the ASAC-CICD is designated by the Inspector General as the Primary Emergency Coordinator. The Primary Emergency Coordinator reports to the AIGI – Threat, Agent Safety and Sensitive Investigations Directorate and keeps the Alternate Emergency Coordinator fully informed on emergency management matters. The Alternate Emergency Coordinator performs all primary duties in the Primary Emergency Coordinator's absence.

120.14.1 COOP Plan. CICD is responsible for the content of the COOP plan. The COOP plan establishes procedures to ensure the continued operation of essential

TIGTA functions within 12 hours of having to relocate the TIGTA headquarters element to an alternate operating facility. The plan complies with the National Security Presidential Directive-51/Homeland Security Presidential Directive (NSPD-51/HSPD-20), "National Continuity Policy," of May 4, 2007, and the National Continuity Policy Implementation Plan, of August 31, 2007, which supersedes Presidential Decision Directive 67 and Federal Preparedness Circular 65. CICD also provides guidance to OI divisions regarding the maintenance of their COOP plans.

CICD is also responsible for maintaining and testing of COOP-related equipment and training of TIGTA staff who have roles in the TIGTA COOP plan.

120.14.2 Executive Emergency Transportation Plan. CICD is responsible for planning, maintaining, and implementing the TIGTA Executive Emergency Transportation Program. This program provides for the coordinated transportation necessary for TIGTA leadership during emergency events.

DATE: January 1, 2019

CHAPTER 400 – INVESTIGATIONS

(400)-130 Firearms, Agent Safety and Tactics Program

130.1 Overview.
This section establishes Office of Investigations (OI) policy and procedures regarding the Firearms, Agent Safety and Tactics (FAST) Program. This policy applies to all 1811 job series criminal investigators (special agents) and 1801 job series investigative specialists who are specifically authorized to carry firearms, including supervisors [Assistant Special Agents in Charge (ASACs), Deputy Special Agents in Charge (DSACs), and Special Agents in Charge (SACs)], hereafter referred to as "SAs."

130.1.1 Acronyms Table.

130.2 Authority.
In accordance with the Inspector General (IG) Act, 5 U.S.C. § 8D(k)(1), as amended by the IRS Restructuring and Reform Act of 1998 (RRA 98), Pub. L. No. 105 206, 112 Stat. 685, and Treasury Order 115-01, Treasury Inspector General for Tax Administration (TIGTA) SAs are authorized to carry firearms while conducting official duties. This authority is also documented in TIGTA Delegation Order 21.

See Section 20.10 for peace officer status and scope of employment.
Federal law prohibits persons convicted of domestic violence from possessing firearms. See Section 20.8.

130.3 FAST Program.
The FAST program standardizes the firearms and defensive tactics training that all OI special agents receive. The FAST program consists of two components:

- Firearms Training; and
- Defensive Tactics Training.

See Section 120 for TIGTA's Use of Force Policy.

130.3.1 FAST Program Personnel. Only SAs who have completed the appropriate training and obtained proper certification may be designated to administer OI's firearms and officer safety programs.

130.3.1.2 National FAST Coordinator. The National FAST Coordinator (NFC) is an SA assigned to Technical & Firearms Support Division (TFSD). The NFC must have completed the Federal Law Enforcement Training Centers (FLETC) Firearms Instructor Training Program (FITP), or an approved equivalent course, at the time of appointment. The NFC manages the FAST program and advises the Deputy Inspector General for Investigations (DIGI), through SAC-TFSD, on officer safety policies, equipment, and training.

The NFC, with assistance from the Divisional FAST Coordinators (DFCs):

- Develops and approves all FAST training modules for the divisions;
- Researches, tests, and evaluates firearms, officer safety equipment, defensive tactics equipment, and training;
- Serves as the lead technical advisor concerning TIGTA's compliance with Federal laws and Department of the Treasury, to include TIGTA policies and procedures regarding firearms and officer safety issues;
- Maintains the national firearms and body armor inventories in the Personal Property Management (PPM) and ensures that these inventories are reconciled annually;
- Ensures that adequate firearms, ammunition, and related equipment are available nationwide;
- Conducts periodic review of firearms-related records maintained by DFCs to ensure compliance with TIGTA policies and procedures;
- Prepares annual budget requests and initiates the procurement of firearms and related officer safety equipment;

- Notifies the respective SAC/Director, the Deputy Assistant Inspector General Investigations (DAIGI), and the appropriate Assistant Inspector General for Investigations (AIGI) when SAs fail to qualify;
- Performs liaison activities with FLETC, other agencies, educational institutions, professional organizations, and appropriate vendors regarding officer safety equipment, policies, and training; and
- Oversees the disposal of TIGTA firearms.

130.3.1.3 Divisional FAST Coordinator. Each SAC designates an SA as the DFC. The DFC must have attended, or be scheduled to attend, FITP at the time of designation. DFCs are required to attend periodic refresher training such as FLETC Firearms Instructor Refresher Training Program (FIRTP) at least every five years, consistent with TFSD guidance. The DFC position is a collateral duty. See Section 40.8.

DFCs are responsible for:

- Reading, understanding, and adhering to TIGTA's FAST policy;
- Promptly reporting issues or concerns to the NFC;
- Maintaining officer safety equipment assigned to the division;
- Ensuring that FAST policies and training are properly implemented throughout the division;
- Issuing required officer safety equipment to SAs in their division;
- Advising the divisional SACs on Federal laws and Department of the Treasury policies and procedures pertaining to the issuance and use of officer safety equipment;
- Maintaining officer safety equipment inventories in PPM and reconciling these inventories annually as described in Section 160.14.1;
- Completing required armorer training;
- Performing and documenting routine firearms inspections and maintenance;
- Documenting receipt and use of ammunition;
- Ensuring that special duty and undercover firearms are properly requested from the NFC, that SAs are properly trained in the use of these handguns before issuance, and that these handguns are promptly returned to the NFC;
- Ensuring the timely completion and documentation of required FAST training and firearms qualifications on the TIGTA OI Form 6601, *Firearms and Agent Safety Training (FAST)/Qualification Record*;
- Notifying the NFC and the SAs supervisor when an SA fails to achieve a qualifying score in a quarterly firearms qualification;
- Coordinating defensive tactics training with the Defensive Tactics Coordinator (DTC);
- Providing opportunities for SAs to complete annually required FAST training as described in Section 130.5; and

- Purchasing miscellaneous officer safety equipment as needed.

130.3.1.4 Firearms Instructors. The SAC will designate one or more SAs in each group or post of duty (POD) as firearms instructors (FIs). These SAs must have completed the FLETC FITP, or an equivalent course approved by the NFC, at the time of designation. FIs are required to attend periodic refresher training such as FLETC FIRTP, Advanced Instruction of Marksmanship Training Program, or an equivalent course approved by the NFC every five years consistent with TFSD guidance. The FI position is a collateral duty. See Section 40.8.

FIs are responsible for:

- Reading, understanding, and adhering to TIGTA's FAST policy;
- Promptly reporting any issues or concerns to the DFC;
- Conducting and documenting firearms qualification and other officer safety training on TIGTA OI Form 6601;
- Notifying the DFC and the SAs immediate supervisor when an SA fails to achieve a qualifying score in a quarterly firearms qualification;
- Coordinating firearms/officer safety training with the DFC; and
- Assisting the DFC in the administration of the division's FAST program.

130.3.1.5 Defensive Tactics Coordinator. Each SAC designates one or more SAs as a DTC. If multiple SAs are selected as DTCs, one DTC may be designated as the primary DTC. These SAs must have completed the FLETC Law Enforcement Control Tactics Instructor Training Program. DTCs must attend the FLETC Law Enforcement Control Tactics Refresher Training Program every five years with the approval of the SAC and concurrence of the NFC. The DTC position is a collateral duty. See Section 40.8.

DTCs are responsible for:

- Reading, understanding, and adhering to TIGTA's FAST policy;
- Promptly reporting any issues or concerns to the NFC;
- Maintaining defensive tactics equipment assigned to the division;
- Ensuring that TIGTA policies and training are properly implemented throughout the division;
- Advising the SAC of compliance with Federal laws and Treasury/TIGTA policies concerning the issuance and use of defensive tactics equipment;
- In conjunction with the DFC, maintaining the defensive tactics equipment inventories in PPM and ensuring that these inventories are reconciled annually as described in Section 160.14.1;
- Documenting defensive equipment maintenance;
- Conducting defensive tactics training; and

- Documenting defensive tactics training on TIGTA OI Form 6601, for inclusion in SA's officer safety training file.

130.3.2 Divisional FAST Program Responsibilities. Each SAC is responsible for their division's FAST program. The SAC will assign a DFC, DTCs, and FIs for their division.

The SAC must:

- Read, understand, and adhere to TIGTA's FAST policy;
- Fund periodic refresher training for DFCs, FIs, and DTCs;
- Ensure the DFC is effectively managing the division's FAST program;
- Select qualified SAs to serve as division armorers; and
- Ensure that a succession plan is in place for the division's FAST program.

The SAC must advise the DFC of staffing changes within their division to ensure the DFC has the required officer safety equipment available to assign to the new SAs.

130.4 Firearms Qualification and Training.
Firearms qualification and training must be conducted by the NFC, a DFC or an FI. The SAC may approve the use of non-TIGTA instructors or non-TIGTA trainers, in consultation with the NFC.

130.4.1 Range Safety. While range safety is required of all personnel on a firearms range, DFCs and FIs are primarily responsible for the safety of all personnel during firearms qualification and training.

All SAs must:

- Read, understand, and adhere to TIGTA's FAST policy;
- Know and comply with all range safety rules;
- Inform the FI/DFC if they are physically unable to safely complete firearms training;
- Initial range safety briefing;
- Obey commands from FIs;
- Wear double ear protection and eye protection with wrap around coverage meeting American National Standards Institute (ANSI) Z-87 requirements; and
- Wear appropriate clothing and footwear.

The FI/DFC must:

- Confirm all shooters are physically able to safely complete firearms training;
- Utilize ranges that are adequate and safe for law enforcement training and qualification;

- Utilize a minimum of one FI per six shooters (1:6) on the firing line for handguns and one FI per four shooters (1:4) on the firing line for long guns, unless the range requires a lower ratio, or additional safety considerations are necessary;
- Utilize a minimum of one FI per shooter (1:1) for any training involving live-fire shooting and moving;
- Document SA's failure to follow safety rules in the SA's officer safety training file, notify the SA's supervisor, and arrange for remedial training (contact the NFC for remedial training guidelines);
- Take possession of the SA's firearm if a safety violation occurs that creates a significant concern, and immediately notify the SA's immediate supervisor and the NFC. If the safety violation involves the SAC, immediately notify the NFC who will notify the DAIGI and respective AIGI; and
- Report all incidents that occur during FAST training, including any property damage, to the proper range authorities.

130.4.2 Firearms Qualification. All SAs will qualify with the handgun, shotgun, and rifle quarterly. SAs must qualify with all TIGTA-issued handguns, including special duty and/or undercover handguns, and any TIGTA-approved personally-owned handguns.

If an SA is a member of the undercover cadre, the SA must qualify with his/her assigned undercover handgun each quarter using the undercover qualification course. See Section 130.12.1.

If an SA has been approved to carry a personally-owned handgun, the SA must qualify with this handgun each quarter using the personally-owned handgun qualification course, even if the personally-owned handgun is of the same model of a TIGTA-issued handgun, including special duty and/or undercover handgun. See Section 130.8.5.

SAs must qualify with their TIGTA-issued standard duty handgun and approved personally-owned handgun with no prior warm-up or practice session and while:

- Wearing a ballistic vest;
- Using a TIGTA-issued holster; and
- Using the ammunition the SA will carry (unless range facilities prohibit such use).

SAs who are issued rifle-resistant plates must wear the rifle-resistant plates and their ballistic vest during long gun qualifications. Because of the added weight and bulk of the rifle-resistant plates, it is strongly recommended that SAs wear the plates during handgun qualifications and other firearms training.

130.4.2.1 Temporary Exemption from Firearms Qualification. A DAIGI, AIGI, or the DIGI may temporarily exempt an SA from routine firearms qualification under certain circumstances, such as an extended detail outside of TIGTA. A memorandum will be

placed in the SA's officer safety training file documenting the temporary exemption. The SA will retain possession of his/her TIGTA-issued standard duty handgun.

A temporary exemption from firearms qualification may be granted no more than once during a fiscal year. The authority to grant such an exemption may not be re-delegated.

130.4.2.2 Temporary Waiver from Firearms Qualification. The second-level supervisor may grant a temporary waiver from firearms qualification to an SA who is unable to qualify with his/her TIGTA-issued standard duty handgun because of a temporary medical condition upon receipt of documentation of the medical condition from a physician. See Section 40.4.

A memorandum will be placed in the SA's officer safety training file documenting the temporary waiver. The memorandum should not include any medical information (*e.g.,* doctor's note or information from the note). If the SA is unable to qualify with the TIGTA-issued standard duty handgun, the SA will turn over the handgun to the DFC until the temporary medical condition is resolved, the SA obtains a medical clearance from a physician and the SA successfully completes firearms qualification. The SA will not be permitted to qualify until a medical clearance is obtained from a physician. The SAC will notify the DAIGI, the appropriate AIGI, and the NFC of the temporary waiver.

The SAC/Director is responsible for the following:

- Ensuring that the SA does not possess or use a TIGTA-issued firearm;
- Ensuring that the SA does not conduct any interviews or participate in any enforcement activities until the SA has received a medical clearance and has qualified with his/her duty handgun;
- Temporarily suspending the SA's authorization to use a Government vehicle, if one is assigned, for home-to-work and work-to-home until the SA receives a medical clearance, successfully qualifies with his/her TIGTA-issued standard duty handgun, and resumes conducting investigative case work; and
- Issuing a memorandum to the SA advising that he/she is not authorized to carry his/her personally-owned handgun and/or undercover handgun while on official duty or outside of core duty hours under the auspices of their TIGTA law enforcement authority until he/she achieves a qualifying score with his/her TIGTA-issued standard duty handgun.

In the event that an SA is able to qualify with his/her TIGTA-issued standard duty handgun but unable to qualify with long gun(s) (*e.g.,* shotgun, rifle) due to a medical condition, the SA will provide medical documentation to support a waiver from the specific long gun(s). The SA will not be permitted to qualify with the long gun(s) until a medical clearance is obtained from a physician. The SAC/Director will notify the DAIGI, the appropriate AIGI, and the NFC of the temporary waiver by memorandum. The memorandum from the SAC/Director will document to which long gun(s) the temporary

waiver applies. The SA will retain possession of his/her TIGTA-issued standard duty handgun.

The SAC/Director is responsible for the following:

- Ensuring that the SA does not use or qualify with TIGTA-issued long gun(s) they are not medically qualified to use; and
- Issuing a memorandum to the SA advising that he/she is not authorized to carry the long gun(s) until he/she achieves a qualifying score with the long gun(s).

130.4.2.3 Failure to Qualify with Firearms. Firearms qualification is a condition of employment. SAs are responsible for maintaining the required level of proficiency with all TIGTA firearms. SAs must qualify with the TIGTA-issued standard duty handgun, shotgun, and rifle quarterly, without an initial warm-up or practice session. The FI/DFC conducting the qualification determines whether the SA meets the firearms qualification requirements and documents this determination on the qualification record. See TIGTA OI Form 6601.

If the SA fails to achieve a qualifying score with the handgun, shotgun, or rifle, the SA may shoot the qualification course a second time on the same range day after completing remedial firearms training. Both scores will be recorded on the TIGTA OI Form 6601. If the SA fails to achieve a qualifying score after remedial firearms training, the SA will be required to relinquish his/her TIGTA-issued standard duty handgun to the FI/DFC at the end of the training day. The SA will not be reissued a handgun until completing additional retraining and successfully achieving a qualifying score with his/her issued handgun(s).

See Section 130.4.2.3.1 for failure to qualify with a personally-owned firearm.

The FI/DFC administering the training session will be responsible for directing the SA to relinquish his/her handgun. The FI/DFC will, without undue delay, notify the SAs immediate supervisor, who is responsible for securing the SA's credential, badges, and other officer safety equipment as soon as practical. Additionally, the FI/DFC is responsible for the following:

- Notifying the SA's immediate supervisor and the NFC that the SA is no longer in possession of a TIGTA-issued handgun;
- Notifying the SA's immediate supervisor and the NFC that the SA can no longer utilize the shotgun and/or rifle;
- Documenting in a memorandum to the SAC/Director the circumstances requiring the SA to relinquish his/her handgun;
- Documenting in a memorandum to the SAC/Director the remedial training program that will be administered for the SA; and

- Arranging remedial training at the earliest possible opportunity.

The DFC will maintain the memorandum in the SA's officer safety training file, and provide a copy to the NFC via e-mail (*TIGTA Inv TFSD).

The second-level supervisor is responsible for the following:

- Ensuring that the SA does not possess or use a TIGTA-issued firearm with which the SA has not qualified;
- Ensuring that the SA does not conduct any interviews or participate in any enforcement activities until the SA has qualified with his or her duty handgun;
- Temporarily suspending the SA's authorization to use a Government vehicle, if one is assigned, for home-to-work and work-to-home until such time as the SA successfully qualifies with a handgun and resumes conducting investigative case work;
- Issuing a memorandum to the SA advising that he/she is not authorized to carry his/her personally-owned handgun while on official duty or outside of core duty hours under the auspices of his/her TIGTA law enforcement authority until he/she achieves a qualifying score; and
- Ensuring that the SA participates in the remedial firearms training program developed by the NFC/DFC for the SA.

Upon failing to achieve a qualifying shotgun or rifle score, the SA will be prohibited from using the firearm operationally until completing the remedial firearms training program and the SA successfully achieves a qualifying score.

130.4.2.3.1 Failure to Qualify with Personally-Owned Handgun. If an SA has been approved to carry a personally-owned handgun in addition to the standard duty handgun, the SA must qualify with this handgun each quarter.

If the SA fails to qualify with his/her personally-owned handgun, the FI/DFC will:

- Notify the SA's immediate supervisor and the NFC that the SA failed to qualify with his/her personally-owned handgun.

The second-level supervisor will:

- Issue a memorandum to the SA advising that he/she is not authorized to carry his/her personally-owned handgun while on official duty or outside of core duty hours under the auspices of their TIGTA law enforcement authority until he/she achieves a qualifying score.

130.4.3 Qualification Courses. The TIGTA qualification courses for handgun, shotgun, and rifle are located on the TFSD intranet page. If necessary, an SA may qualify using the FLETC Practical Pistol Course (PPC) in non-successive quarters.

130.4.3.1 Targets Used for Qualification. The International Association for Law Enforcement Firearms Instructor (IALEFI) – "QR" photo targets will be used for firearms qualification.

The U.S. Treasury Transitional Target II target (*i.e.*, FLETC Trans-Tar II) and other Federal Bureau of Investigation "Q" targets may be used if the IALEFI-QR photo targets are unavailable. Scoring of the target is done by using the target's scoring rings and determining the score based on the TIGTA 50-round course. Any law enforcement or military target can be used for approved firearms training modules, but not for firearms qualification.

130.4.4 Special Circumstances. A pregnant SA may decide to continue firearms qualification during her pregnancy. Regardless of her decision, she must provide documentation from her physician supporting her decision, and provide updated documentation from her physician every two months in accordance with the requirements outlined in Section 40.4.

Note: Pregnant SAs who choose to continue qualification are authorized to qualify with, but not carry, nonstandard lead-free ammunition, if available. The NFC must ensure that the non-standard ammunition closely approximates the performance of standard duty ammunition.

130.4.5 Ammunition for Practice. Limited amounts of ammunition will be made available for this purpose. SAs must obtain the ammunition from the FI or DFC and account for such use. SAs must only use agency-issued duty ammunition as well as agency-approved firearms.

SAs that are in the TIGTA Remedial Firearms Program are not permitted to practice live fire outside of core duty hours.

130.4.5.1 Practice Range Facilities. Practice outside of core duty hours may be conducted at military, police, or public use ranges; however, the use of military or police ranges is preferred.

130.4.5.2 Federal Employees Compensation Act. The Federal Employees Compensation Act (FECA) covers SAs engaged in firearms practice outside of core duty hours when the following conditions apply:

- TIGTA-issued firearms and ammunition are used; or

- Approved personally-owned handguns and TIGTA-issued ammunition are used; and
- The SA is wearing approved officer safety equipment.

130.5 Special Agent Safety Training.
In addition to firearms qualification, SAs must successfully complete a variety of FAST training modules during each 12-month training cycle. The NFC will establish annual training requirements and post them on TFSD's intranet site.

The training curriculum will be provided to the SACs one week prior to the start of the yearly training cycle. The training cycle will begin on October 1 and end on September 30. Additional training may be requested by the SACs after consultation with their respective DFCs and DTCs. All FAST training will be approved by the NFC.

All training will be documented on TIGTA OI Form 6601 by the FI/DFC.

Each SA is required to receive quarterly training presentations on:

- Firearms safety; and
- Treasury and TIGTA policies on use of force.

Each SA is required to receive annual training presentations on:

- TIGTA policy on firearms security; and
- Baton and oleoresin capsicum (OC) familiarization.

130.5.1 Expandable Baton Training. Initial baton training consists of approximately six hours of formal training. All baton instructors must have received baton instructor training from FLETC or the baton vendor.

The FAST program requires annual refresher training on the use of the expandable baton. SAs that have not completed annual refresher training by the end of the fiscal year will not be permitted to carry a baton. The DTC must notify the SAC for appropriate action. DTCs must document all baton training in the SA's officer safety training file.

130.5.2 Oleoresin Capsicum Aerosol Training. Each SA is required to receive annual familiarization training on the use of OC. All SAs who choose to carry OC aerosol as an intermediate force weapon must complete initial OC aerosol training that includes exposure to OC aerosol.

Initial OC aerosol training consists of approximately two hours given by either:

- An instructor who has received OC aerosol instructor training given by an appropriate school or academy, such as FLETC; or
- An instructor who is employed by an appropriate training school or academy.

Upon completion of training, the SA must provide a memorandum to the SAC that includes:

- Date of exposure;
- Place of exposure; and
- Instructional setting in which they received the OC aerosol training.

Once the SAC receives documentation of the OC aerosol training, the SA may carry OC aerosol as an intermediate force weapon in addition to the baton.

Continued authority to carry OC aerosol requires that each SA annually complete the defensive tactics refresher training of the FAST program, which includes a block of instruction on OC aerosol. This training does not require additional exposure to OC aerosol, but instead involves completion of inert OC aerosol exercises. SAs that have not completed OC refresher training by the end of the fiscal year are not authorized to carry OC aerosol until such time as the refresher training is completed.

SAs with medical conditions that preclude exposure to OC aerosol must notify the SAC of this condition and refrain from carrying OC aerosol. During the period that medical conditions preclude exposure to OC aerosol, each SA must remain certified to carry an expandable baton as an intermediate force weapon. SAs can again carry OC aerosol when the medical conditions that precluded such carry ceases, and training requirements have been met.

DTCs must document all OC training in the SA's officer safety training file.

130.6 Special Agent Officer Safety Training Files.
DFCs must maintain an officer safety training file for each SA containing the following:

- Qualification records;
- Firearms training records;
- Officer safety training records; and
- Equipment inventory.

130.6.1 Documentation of Training. Document all firearms qualifications and FAST training on TIGTA OI Form 6601. Annual training requirements are posted on TFSD's intranet site.

The DFC will prepare a memorandum to the SAC/Director detailing the results of each quarterly qualification/training cycle and provide a copy to TFSD by uploading it to the divisional FAST training SharePoint site.

The memorandum must include the following:

- Qualification scores of all SAs;
- Names of all SAs who are authorized to carry a personally-owned firearm and denote whether or not those SAs have qualified with their personally-owned firearm;
- Names of all SAs who are issued rifle-resistant plates and denote whether or not those SAs have completed firearms qualifications while wearing the rifle-resistant plates; and
- Whether or not members of the undercover cadre qualified with the issued undercover firearm. The memorandum will not identify the undercover member(s).

The memorandum is due by the 5th business day after the quarter ends on December 31, March 31, June 30, and September 30.

The DTC will prepare a memorandum to their divisional SAC/Director detailing the results of defensive tactics training completed by each SA during the calendar year and provide a copy to the NFC via e-mail to the TFSD Inbox (*TIGTA Inv TFSD). The memorandum is due by October 5th of each calendar year.

The SAC must document in the SA's officer safety training file whenever the SA is excused from completing mandatory annual FAST training and notify the DAIGI, appropriate AIGI, and NFC. If an SA begins employment with TIGTA during the training year, the SA must complete the remaining required FAST modules for that year.

130.6.2 Records Retention. Documentation of officer safety training is kept for the length of the SA's employment with TIGTA. When an SA transfers to another division, the training records are transferred via traceable delivery such as UPS to the receiving division. When an SA leaves TIGTA, send the original officer safety training file to the individual's most recent supervisor while employed at TIGTA for inclusion in the individual's drop file. If requested, provide copies of the records to the individual and/or the new agency.

Officer safety training files will be destroyed three years after the date of the SA's separation or retirement from TIGTA.

130.6.3 Security of Records. Maintain officer safety training records in a secure area. SAs may review, but not change, their training records.

130.7 Special Agent Safety Kit.
Special agent safety kits are issued to all SAs. See TIGTA OI Form 6602, *Annual SA Safety Kit Inventory*.

SAs will initial and date TIGTA OI Form 6602 and sign TIGTA OI Form 1930, *Custody Receipt for Government Property*, when issued equipment. SAs are responsible for the items in the kit, the serviceability of the items, and the retention of this equipment during their employment with TIGTA. SAs will retain their assigned officer safety kit when transferring between divisions.

The DFC will conduct an annual inventory of the office safety equipment assigned to each SA using TIGTA OI Form 6602. SAs will contact the DFC for replacement items.

130.8 Firearms.
TIGTA maintains an inventory of firearms that includes standard duty handguns, special duty handguns, shotguns, rifles, training firearms, and firearms modified to fire non-lethal training ammunition (NLTA).

130.8.1 Standard Duty Handguns. Each SA will be issued one standard duty handgun.

130.8.2 Special Duty Handguns. Special duty handguns include an inventory of undercover and training handguns. The NFC maintains the inventory of special duty handguns. The DAIGI, or the appropriate AIGI, after consulting with the NFC, may approve the issuance of special duty handguns to meet operational needs. If issued, the DFC must return the special duty handgun to the NFC at the conclusion of the assignment.

130.8.3 Long Guns. A long gun (*e.g.*, rifle, shotgun) is a defensive weapon utilized to enhance the safety of SAs and others during law enforcement operations. Only approved ammunition, accessories, magazines, and optical sighting devices purchased by, or approved by, the NFC are authorized for use with TIGTA long guns.

130.8.3.1 Deployment of Long Guns. The SA who is considering deployment of a long gun should discuss this matter with the ASAC prior to preparation of the operational plan. ASAC approval is required for the deployment of long guns during an enforcement operation. This approval authority may not be re-delegated. Under exigent circumstances, such as an active threat situation, the SA may deploy a long gun without ASAC approval. The ASAC will be notified as soon as it is safe to do so.

130.8.3.2 Consideration Criteria for Deployment. Deploying the long gun may be appropriate if the law enforcement activity is planned in a rural or remote area.

Deployment in urban areas is allowed if operationally required and approved. Careful consideration should be given to deploying a rifle in a confined space such as an office building, which may not be appropriate.

Consider the following for long gun deployment:

- Subject has access to body armor and/or firearms;
- Subject has received military and/or police training;
- Subject has been involved in assaults against employees of Government agencies at the Federal, State, county, and/or local level;
- Subject has made specific threats of violence against employees of Government agencies at the Federal, State, county, and/or local level;
- Subject is a member of, or is closely associated with, criminal organizations known to be violent, religious extremists known to be violent, paramilitary groups, or terrorist groups; and
- The need exists for perimeter security for a law enforcement activity.

130.8.4 Training Firearms. Deactivated training firearms are used in training situations where firearms are pointed at other individuals. These firearms are:

- Incapable of chambering or firing any ammunition; or
- Capable of chambering and firing only (NLTA).

Training firearms that are either permanently or temporarily deactivated will be clearly identified by red markings such as red painted grips and/or red tape wrapped around the grips or barrel.

Firearms modified for NLTA will be marked with blue paint or tape.

When NLTA is used, an instructor who has completed the FLETC Instructional Techniques for Non-Lethal Training Ammunition (ITNTA) or similar instructor training must be present. Training with NLTA must be conducted in accordance with FLETC ITNTA standards.

Weapons and ammunition (*e.g.*, firearms, ammunition, knives, batons, OC, etc.) are not permitted in the training area. Only conduct such training in a facility or area that has been specifically designated for use of NLTA or that can be suitably controlled for this training.

130.8.5 Personally-Owned Firearms. SAs may carry an approved personally-owned handgun outside of the SA's core duty hours and as a secondary (*i.e.*, "back-up") handgun during core duty hours. Prior to carrying a personally-owned handgun, SAs must obtain written approval from their SAC through their ASAC. The request should

be submitted to the NFC via the TFSD Inbox (*TIGTA Inv TFSD). The NFC will facilitate a criminal history check of the requesting SA. If the SA intends to purchase the handgun from a Federally-licensed firearms dealer, the SA will also be required to submit an Agency Certification Letter for the DIGI's signature. The DFC will place the approval memorandum in the SA's officer safety training file.

Once the request is approved, the personally-owned handgun must be inspected by the NFC, DFC, or an FI to determine if it is suitable for firing and the handgun will be inspected before each qualification. SAs must qualify with the personally-owned handgun each quarter.

130.8.5.1 Failure to Achieve Qualifying Score with Personally-Owned Handgun.

If the SA fails to achieve a qualifying score with his/her personally-owned handgun, the FI/DFC will:

- Notify the SA's immediate supervisor and the NFC that the SA failed to qualify with his/her personally-owned handgun.

The second-level supervisor will:

- Issue a memorandum to the SA advising that he/she is not authorized to carry his/her personally-owned handgun while on official duty or outside of core duty hours under the auspices of their TIGTA law enforcement authority until he/she achieves a qualifying score.

If the SA fails to achieve a qualifying score with his/her TIGTA-issued standard duty handgun, the SA will not be authorized to carry his/her personally-owned handgun while on official duty or outside of core duty hours under the auspices of their TIGTA law enforcement authority.

If the SA is a member of the undercover cadre and the SA's approved personally-owned handgun is the same model as the undercover handgun, the SA is required to qualify with each handgun using the firearms qualification course designated for each handgun.

Contact TFSD for a list of approved personally-owned handguns and holsters. See Section 130.11.1.

An approved personally-owned handgun will not be carried in lieu of the TIGTA-issued standard duty handgun during core duty hours. See Section 130.13.

130.8.6 Non-TIGTA Owned Firearms for Evaluation. The NFC may approve the use of non-TIGTA owned firearms for evaluation purposes only. The non-TIGTA owned firearm will only be used for evaluation purposes after the NFC has approved its use

and the NFC, DFC, or FI has inspected the firearm and determined it to be suitable for firing.

130.9 Intermediate Force Weapons.
The Treasury Use of Force Policy requires the appropriate use of less than lethal force. SAs are issued intermediate force weapons consistent with these policies to be used in performance of official duties.

TIGTA issues two types of intermediate force weapons. The expandable baton is the primary intermediate force weapon and must be carried, or be readily accessible, whenever an SA is carrying a TIGTA firearm. OC aerosol may be carried in addition to, but not in lieu of, the expandable baton. TIGTA SAs will not carry or use intermediate force weapons, such as OC aerosols or expandable baton, as a substitute for a firearm. OC aerosols and expandable batons are to be issued and used only as described in this section.

Spraying a person with an OC aerosol or striking a person with a baton constitutes a use of force. See Section 120.

130.9.1 Oleoresin Capsicum Aerosols. OC aerosols will contain a 5-6% oleoresin capsicum solution using either a spray or stream delivery system. The aerosol will not contain any active chemical agent other than oleoresin capsicum. Foam type OC aerosols are prohibited. SAs will only carry OC aerosols approved and issued by TIGTA. Do not use OC aerosols past the manufacturer's expiration date printed on the container.

130.9.1.1 Use of Oleoresin Capsicum Aerosols. SAs may spray another person with an OC aerosol when lesser measures, including verbal persuasion and unarmed restraining techniques, have proven ineffective, or are likely to prove ineffective, to stop the person and:

- The person physically assaults, or attempts to physically assault, the SA or another person; or
- The person resisting arrest indicates, by words or actions that they intend to physically assault the SA or another person during the arrest.

When spraying a person, direct the center of the spray or stream in the area of the person's nose. Use the minimum force necessary. Cease spraying a person when the above criteria no longer apply.

As soon as possible after use of OC:

- Secure the person being sprayed with appropriate restraints;
- Flush the affected areas with cold water; and

- Obtain prompt medical attention.

If an SA sprays a person with an OC aerosol, report this incident as a use of force as described in Section 120. This does not apply to formal training situations using SAs as subjects.

Animals may be sprayed with an OC aerosol when the SA believes the animal is a danger to the SA or other persons.

130.9.1.2 Carrying Oleoresin Capsicum Aerosol. An SA must carry OC aerosols in a discreet, secure, and readily accessible manner in a TIGTA-issued or approved OC carrier. SAs may draw the OC aerosol and hold it in their hand if they believe its use is imminent.

Do not leave OC aerosols within easy access of unauthorized persons. Do not leave OC aerosols in vehicles.

SAs flying aboard aircraft must place OC in checked baggage per Federal Regulation 49 C.F.R. § 175.10(a)(9), which states that "one self-defense spray… not exceeding 118 ml (4 fluid ounces) by volume, that incorporates a positive means to prevent accidental discharge may be carried in checked baggage only."

130.9.1.3 Storage, Shipment, and Disposal of Oleoresin Capsicum Aerosols. SAs must store and ship OC aerosols in compliance with applicable Federal, State, and local laws and in compliance with the OC aerosol manufacturer's standards.

When shipping OC aerosols:

- The shipper must have completed the appropriate Department of Transportation (DOT) hazardous shipping training and ship the OC in compliance with the DOT requirement and all markings; and
- Use only ground transportation. Never use air transportation.

Dispose of OC aerosol containers by spraying any remaining contents in a safe and appropriate area and then discarding the empty container in a suitable area, such as a landfill, where the container is not readily accessible to another person. Contact the DTC or DFC for complete disposal instructions. Never incinerate OC aerosol containers.

Contact the NFC if any special disposal problems arise.

130.9.2 Expandable Batons. Expandable batons for use during confrontational interviews, protective operations, and enforcement activities must meet the following specifications:

- Constructed of metal with bonded rubber handles;
- No more than 21 inches in total length when fully extended; and
- Extended by the use of inertia and not by mechanical devices such as springs.

The striking portion of the baton will be free of sharp, pointed, or highly abrasive areas. Batons will not be modified except that the retaining spring may be adjusted to facilitate proper opening and closing of the baton. Do not attach flashlights to batons.

Expandable batons may only be issued and used as described in this section.

130.9.2.1 Lightweight Expandable Batons. SAs are issued lightweight batons in addition to their regular equipment. These batons will not be used during confrontational interviews, protective operations, and enforcement activities.

130.9.2.2 Use of Expandable Batons. SAs may strike another person with a baton when lesser measures, including verbal persuasion, and unarmed restraining techniques, have proven ineffective or are likely to prove ineffective, to stop the person and:

- The person physically assaults, or attempts to physically assault, the SA or another person; or
- The person resisting arrest indicates, by words or actions that they intend to physically assault the SA or another person during the arrest.

Use the minimum force necessary. Cease striking a person with a baton when the preceding criteria no longer apply.

Strike an assailant at the major muscle groups of the arms or the legs. Avoid strikes to the trunk of the body. **Do not** intentionally strike the head or the neck since serious injury or death may occur.

130.9.2.3 Use of Expandable Baton as a Non-Impact Weapon. A baton may be used as a non-impact weapon when applied to suitable pressure points on a subject's body. If an SA strikes a person with a baton:

- Ensure that prompt medical attention is made available to that person; and
- Report this as a use of force incident as described in Section 120.3.

130.9.2.4 Carrying Expandable Batons. Always carry batons in a discreet, secure, and readily accessible location. Use of baton carriers is optional. SAs may draw the baton if they believe its use is imminent.

130.10 Body Armor.
SAs will use only TIGTA-supplied or approved body armor. Each SA will be issued body armor that has been manufactured to provide the appropriate level of protection against threats as determined by the NFC.

The DFC is responsible for:

- Ensuring that SAs are measured properly for body armor;
- Issuing body armor/rifle-resistant plates to the receiving SA;
- Obtaining a signed Form OI 1930 from the SA to be maintained in the SA's officer safety file;
- Providing a copy of the completed Form OI 1930 to the NFC within 10 days;
- Notifying the NFC of receipt of the body armor/rifle-resistant plates within 10 days;
- Adding the body armor/rifle-resistant plates to the divisional inventory in PPM; and
- Notifying the NFC within one year of the body armor's warranty expiration date (*i.e.,* typically five years from the date of manufacture).

When an SA receives his or her body armor/rifle-resistant plates from the manufacturer, the SA will report to the DFC within five duty days that:

- The body armor is the correct type and it fits properly; and
- The date of manufacture and the serial number indicated on the armor.

130.10.1 Damaged Body Armor. Immediately withdraw from service any body armor that has been damaged. Notify the SAC and NFC of any body armor that is unserviceable for any reason (*e.g.*, mildew, mold, oil, chemical stains, size, fit). The NFC will authorize the return of damaged body armor to determine if it should be permanently removed from service. Contact the NFC regarding the disposal of outdated or unserviceable body armor.

130.10.2 Transferring Body Armor. TIGTA SAs who transfer to another Federal law enforcement agency may request approval to have their body armor transferred to their new agency. New TIGTA SAs must request approval for use of body armor purchased by another law enforcement agency. Body armor purchased by another Federal agency continues to be the property of the U.S. Government. Contact the NFC to initiate these transfers. Rifle-resistant plates and low visibility body armor will not be transferred and will be retained by TIGTA.

130.10.3 Use of Body Armor. The routine wearing of body armor is encouraged. SAs are required to wear body armor when performing enforcement activities or protective operations including, but not limited to the following:

- Executing arrest or search warrants;
- Responding to an active threat;
- Protective details;
- Conducting interviews of subjects in assault/threat cases; and
- Performing surveillance of, or making contact with, individuals who may be dangerous.

SAs will wear body armor during firearms qualifications to demonstrate that they have sufficient firearms handling skills while wearing their ballistic vests. Because the low visibility body armor provides the same level of protection as the standard issued body armor, it may be worn during firearms qualification. FIs should also inspect body armor for proper fit and serviceability during this time.

Do not shoot body armor as part of any training or evaluation except as authorized by the SAC and the NFC.

SAs have the option of requesting rifle-resistant plates. Rifle-resistant plates may impact mobility as a result of the added weight and bulk. All SAs who are issued these plates are required to wear them, in addition to body armor, during quarterly long gun qualification. The decision to wear rifle-resistant plates during enforcement activities is left to the SAs' discretion, but it is strongly recommended that they be worn during enforcement activities.

Note: Rifle-resistant plates do not replace body armor and will be worn in conjunction with the ballistic vest during firearms qualification (See Section 130.4.2) and enforcement activities, if utilized.

130.10.3.1 Body Armor for IRS Employees During Armed Escorts. Body armor having serviceable dates may be provided to IRS employees for use during armed escorts with ASAC approval. IRS employees are not permitted to keep or store the body armor overnight. The case agent will ensure the body armor is returned at the conclusion of the armed escort. Contact the NFC if body armor is needed for an armed escort.

130.10.4 Body Armor Storage. Body armor should be stored lying flat and not exposed to direct light. SAs should not leave body armor (ballistic vest, low visibility armor, and rifle-resistant plates) unattended in a motor vehicle for extended periods (*e.g.,* overnight).

130.11 Special Agent Safety Equipment.
Upon completing the FLETC Criminal Investigator Training Program (CITP), each SA will be permanently assigned officer safety equipment. The SA is responsible for safeguarding the equipment. SAs must immediately notify the appropriate FI/DFC when any item of officer safety equipment is lost or in need of replacement or repair.

130.11.1 Holsters. Carry handguns in a safe, discreet, and secure manner. Each SA is issued a strong-side hip holster that meets the following specifications:

- Constructed of leather, nylon, or composite material;
- Designed to be securely attached to a belt;
- Employs a positive retention device or thumb break capable of safely holding the firearm when holstered and when inverted;
- Designed and/or molded to fit the handgun being carried and marked or described as such by the manufacturer;
- Covered trigger guard;
- Permits the handgun to be drawn and re-holstered using one hand;
- Permits drawing the handgun using the support hand;
- Described by the manufacturer as suitable for concealed police use; and
- Capable of safe utilization during qualification and training (*e.g.,* muzzle does not point in the direction of other persons).

Any holster that requires the use of the trigger finger to release the firearm from the holster is not approved for use. Holsters should not be modified unless approved by the NFC.

130.11.1.1 Optional Holsters. Optional holsters must meet the same criteria established for strong-side hip holsters and SAs must qualify with the optional holster before carrying it for duty. The FI/DFC will document qualification with the optional holster in the SA's officer safety training file. The NFC must approve any optional holster prior to purchase or use. An optional holster must be purchased with divisional funds and approved by the NFC before use.

Contact the NFC for specifications and approval of special duty and undercover handgun carry methods.

130.11.1.2 Ankle Holsters. SAs may utilize a TIGTA-approved ankle holster to carry a TIGTA-approved personally-owned handgun as a secondary or "back-up" handgun. Prior to carrying the ankle holster, SAs must complete a familiarization course with the holster. SAs must complete the familiarization course annually to continue carrying the ankle holster. Upon completion of the familiarization course, the FI/DFC will document completion on TIGTA OI Form 6601. This familiarization documentation must appear in the quarterly qualification memorandum once the qualification course is completed.

130.11.2 Handcuffs and Restraining Devices. Handcuffs and restraining devices used by SAs will meet the standards described in this section.

130.11.2.1 Handcuffs. SAs will only carry TIGTA-issued handcuffs and restraining devices. SAs are required to carry their TIGTA-issued handcuffs when carrying a

firearm on official duty. SAs will not carry temporary hand restraints in lieu of handcuffs when carrying a firearm on official duty. Handcuffs must:

- Be constructed of steel or steel and aluminum;
- Be either chain or hinged type; and
- Have either a high security lock or a standard lock with a double lock.

130.11.2.2 Restraining Devices. Other restraining devices such as temporary hand restraints (*e.g.*, disposable "flex cuffs"), belts and leg restraints, may be used and will be specifically designed and suitable for such purposes.

130.11.2.3 Handcuff and Restraining Device Use. SAs are responsible for the safety and care of persons in their custody. Always handcuff and search persons taken into custody. Search all handcuffed persons when custody is transferred from one law enforcement officer to another. Search all areas where a person in custody will be placed (*e.g.*, GOV, interview room) before and after movement.

Temporary hand restraints should only be used until metal handcuffs can safely be applied. When temporary hand restraints are carried and used, ensure that a cutting tool is available for safe removal.

Do not use makeshift restraining devices except in emergency situations.

130.12 Firearms Issuance.
Before an SA is provided a TIGTA-issued handgun, the SA must successfully complete:

- Semi-automatic pistol training at the FLETC CITP, or equivalent semi-automatic pistol training totaling at least 24 hours;
- Qualify with their issued handgun or other TIGTA-owned handgun pursuant to Section 130.4; and
- Meet TIGTA intermediate force weapon training requirements pursuant to Section 130.9.

130.12.1 Undercover Firearms. The SAC may authorize an SA to carry an undercover firearm for undercover assignments and training for undercover assignments. This authorization expires when the undercover assignment or training ends. Undercover firearms will not be issued, or carried in lieu of, standard duty handguns. SAs that have been authorized to carry undercover firearms must qualify with the undercover firearms quarterly.

The DFC and FI must ensure that the SA is familiar with the functioning and safe handling of the undercover firearm and document that the SA has qualified with it. The SA must demonstrate his/her proficiency in handling the firearm and shooting the firearm in the manner in which it will be carried during the undercover operation.

Note: Do not disclose the make, model, or serial number of TIGTA's undercover firearms to individuals outside TIGTA.

130.12.2 Shotguns and Rifles. Shotguns and rifles are not individually issued to SAs. Shotguns and rifles are assigned to the ASAC or DFC in PPM. Each POD is assigned a shotgun and a rifle. The DFC will keep an unassigned handgun, shotgun, and rifle in inventory. ASACs may authorize the use of shotguns and rifles for specific enforcement operations.

130.13 Carrying of Firearms.
Unless prohibited from doing so under a specific provision of this section, SAs are authorized to carry TIGTA-issued handguns and TIGTA-approved personally-owned handguns at all times to facilitate the expeditious performance of their law enforcement duties outside of core duty hours. For the purposes of this policy, core duty hours refers to the eight-hour day an SA works that is not considered LEAP hours.

All SAs will carry their TIGTA-issued standard duty handgun and related equipment during core duty hours unless:

- The SA is in an undercover capacity;
- The SA is prohibited by policy from doing so; or
- When judgment or policy dictates that non-carry is appropriate (*e.g.*, Federal courthouse, prison, or similar facility).

130.13.1 Carrying Firearms When Conducting Investigative Activities. SAs must carry their standard-issued handgun and the following equipment when conducting investigative activities:

- Expandable baton;
- TIGTA-issued holster;
- Handcuffs with key;
- Enforcement badge and credentials;
- Extra magazine(s) fully loaded with duty ammunition; and
- Cellular telephone and/or TIGTA-issued radio.

SAs are authorized to carry the TIGTA-issued lightweight expandable baton and handcuffs when not engaged in confrontational interviews, protective operations, or enforcement activities.

130.13.2 Carrying an Approved Personally-Owned Handgun. SAs who are authorized to carry an approved personally-owned handgun outside of core duty hours must carry the following equipment:

- Expandable baton or lightweight expandable baton;
- TIGTA-issued holster;
- Handcuffs and key, lightweight handcuffs and key, or alternate restraining device as described in Section 130.11.2;
- Credentials; and
- Cellular telephone.

130.13.3 Exemption from Carrying a Handgun. SAs acting in an undercover capacity are exempt from the requirement to carry, or have readily accessible, their issued handgun and related equipment. SAs are not required to carry a handgun when judgment of unique circumstances dictates that non-carry is appropriate (*e.g.*, Federal courthouse, prison, or other similar facility).

130.13.4 Prohibition on Carrying a Handgun. SAs are not authorized to carry a handgun when:

- Qualification is not current (requires SAC notification and a Memorandum of Waiver to carry);
- Prohibited by TIGTA policy;
- Prohibited by their SAC (*e.g.*, medical or disciplinary status);
- Temporary medical condition makes the SA unable to safely and effectively operate the firearm; or
- Traveling outside the United States, unless authorized by the host Government.

SACs, in consultation with the DAIGI or the appropriate AIGI, may temporarily suspend or restrict the authority of an SA to carry a handgun and related equipment, enforcement badge, credentials, and/or use of a government vehicle. When an SA is prohibited from carrying a TIGTA-issued handgun, related equipment, enforcement badge, credentials, and/or use of government vehicle, the supervisor will take possession of the handgun and equipment, and provide it to the appropriate custodian for safekeeping until the prohibition is lifted (*e.g.*, FI or DFC with access to a gun safe). During the time the SA is prohibited from carrying a TIGTA-issued handgun, the SA is not authorized to carry a personally-owned handgun for official business or outside of core duty hours under the auspices of their TIGTA law enforcement authority.

SAs will return their TIGTA-issued handgun(s) to the appropriate FI/DFC when in non-pay status. Non-pay status includes suspensions, leave without pay, etc.

130.13.5 Firearms Carry Conditions. All handguns, including approved personally-owned handguns, will be carried in a TIGTA-issued holster, with the chamber loaded, and a full magazine inserted in the handgun.

Shotguns will be carried using two hands or a sling with the:

- Chamber empty;
- Safety on; and
- Magazine tube fully charged with either buckshot or slug.

Only chamber a round when the following conditions apply:

- The SA is physically carrying the shotgun; and
- The SA can articulate that the imminent discharge of the shotgun may be warranted.

Note: A loaded shotgun may fire if dropped or struck with enough force.

Rifles will be carried with a sling with the:

- Chamber loaded;
- Safety on; and
- Magazine charged in accordance with TIGTA training.

When appropriate, SAs are permitted to display a firearm in order to avoid its actual use.

130.13.6 Carrying Firearms on Aircraft. The regulations of the Department of Homeland Security, Transportation Security Administration (TSA), provide information and guidance concerning carrying firearms and transporting passengers under the control of armed law enforcement escorts (see 49 C.F.R. §§ 1540.111 and 1544.219).

All SAs are required to complete TSA's Law Enforcement Officer Flying Armed Training Course and annual refresher training on flying armed. Additionally, SAs must receive periodic training required by TSA concerning changes to FAA policies and regulations concerning flying while armed. TIGTA SAs will fly armed when traveling on official business unless the purpose of such official travel precludes use of a firearm during the assignment. Since SAs are authorized to carry TIGTA-issued handguns and approved personally-owned handguns at all times except when prohibited for a reason specified in Section 130.13.4 of this section, SAs are authorized to carry their TIGTA-issued handgun and approved personally-owned handgun aboard an aircraft when flying for personal reasons in the United States. SAs are not permitted to place their handgun in checked-baggage. TSA regulations require that the SA present credentials when required and conceal the handgun.

When flying armed, notify appropriate airline officials at the check-in counter. SAs will complete the flying armed paperwork provided by the airline. As a general rule, armed SAs are in one of the following categories when in travel status:

- Armed individual traveling alone, occasionally without baggage;
- Armed, transporting a non-dangerous prisoner;
- Armed, transporting a dangerous prisoner;
- Armed escort accompanying a dignitary;
- Armed, conducting a surveillance on suspect; or
- Armed escort for protection of a witness or informant.

In the event of a disturbance aboard the aircraft, do not take any action unless the flight crew specifically requests it. For aircraft hijackings or other life-threatening situations, do not take action if there are Federal air marshals (FAMs) onboard unless they specifically request assistance. For aircraft hijackings or life-threatening situations when there are no FAMs aboard, take the necessary action to prevent loss of life or serious physical harm. Any action taken must be in accordance with the Treasury Use of Force Policy. See Section 120.3 of this chapter.

130.13.7 Display of Firearms. When in the presence of the public, only draw your handgun in a situation that is threatening or potentially threatening. Shoulder firearms *(i.e.*, long guns) may be displayed as necessary.

Unconcealed handguns may be worn while in TIGTA offices and work areas. However:

- Do not display firearms in situations and areas where good judgment dictates otherwise; and
- Do not unnecessarily display firearms in areas open to public view.

130.14 Firearms Safety.
SAs must always adhere to the following four basic safety rules:

- Treat all firearms as though they are loaded; check each firearm visually, and physically (as applicable) before declaring it unloaded;
- Never point a firearm at any individual that you are not willing to shoot or at anything that you are not willing to destroy. Always be aware of your muzzle and point firearms in the safest possible direction;
- Keep fingers off of the trigger and outside the trigger guard until you are ready to fire; and
- Know your target, backstop, and what is beyond. Know what is between you and the target. Never shoot at anything that you have not positively identified.

130.14.1 Firearms and the Consumption of Alcohol or Medication. SAs will not consume alcoholic beverages while carrying a firearm. After alcohol consumption, SAs must refrain from carrying a firearm until such time that the SA is able to safely and effectively operate the firearm.

SAs will not carry a firearm while under the influence of any drug or medication that impairs their ability to safely and effectively operate the firearm. SAs taking either prescription or over-the-counter medication, which may impair his/her ability to safely and effectively operate the firearm, must report the impairment to his/her immediate supervisor.

The SAC may authorize the consumption of alcohol while carrying a firearm during approved undercover activities. When the consumption of alcohol while armed is approved as an operational requirement, SAs must do so in moderation.

130.15 Firearms Storage and Security.
Do not leave firearms unsecured. SAs will take every reasonable precaution to prevent the loss or theft of firearms and related equipment.

Presidential orders and Treasury policies require that each TIGTA firearm be issued with a child safety device. Only TFSD-approved child safety devices will be used. Child safety devices will only be used with unloaded firearms. SAs must follow manufacturer's instructions when using said child safety devices. Cable gun locks are the only TFSD-approved child safety device.

130.15.1 Unattended Firearms. At a minimum, unattended firearms must be secured by one or more of the following:

- Installing a TFSD-approved child safety device;
- Placing the firearm in a commercially available lock box or container providing appropriate security for firearms; or
- Placing the firearms in a TIGTA-approved storage container.

TIGTA provides approved storage containers for keeping firearms secure, both at the office and at home. TIGTA-issued firearms storage containers are accountable property and must be returned when the SA separates from TIGTA.

When a handgun is not being worn by a SA, it should be secured as follows:

- Locked in an office day safe (temporary "on-duty" storage);
- Locked in an office gun safe (long-term storage);
- Locked in a home security container; or
- Stored with a child safety device.

When not in use, long guns should be locked in an office gun safe. If the long gun is in the possession of an SA during transit that is not related to an enforcement activity (*e.g.*, traveling to the range), it should be placed in a padlocked gun case or stored in an NFC-approved firearms safe. Long guns should be placed in a padlocked, hard-shell shipping case during shipment.

Firearm	Location	Container
Handgun	Office	Day safe (on duty) Gun safe (long-term)
	Home	Home security container
Shotgun	Office	Gun safe
	Transit	Lockable case or secured firearms safe
Rifle	Office	Gun safe
	Transit	Lockable case or secured firearms safe
All Types	Shipment	Locked hard shell case

Do not store loaded handguns overnight in an office day safe as these containers are intended only for "on duty" security of handguns when the office is occupied by other OI personnel. Any firearm stored in a TIGTA gun safe must be **unloaded** since storage in these containers is long-term and involves multiple firearms.

130.15.2 Firearms Handling Area. Each POD must have a designated firearms handling area equipped with a commercial bullet trap. All loading, unloading, and handling of firearms must be done in the designated firearms handling area. When loading or unloading a firearm, always point the muzzle of the firearm at the center of the commercial bullet trap.

The firearms handling area will be configured with adequate lighting and privacy so that the muzzle of the firearm being handled is:

- Not pointed in the general direction of an occupied area of the office;
- Not pointed at an easily penetrable barrier such as a thin wall or partition; and
- Not pointed at an obstacle that could cause a ricochet into an occupied area of the office.

130.15.3 Firearms Security Containers. Each office will be equipped with an approved firearms security container (gun safe). These containers are for long-term storage of firearms and must meet one or more of the following standards:

- General Services Administration (GSA) approved security containers as labeled by the manufacturer;
- GSA approved Class # 5 Safe; or
- Approved commercial-grade gun safe (UL rating of class #2 / Sargent & Greenleaf dial or electronic combination lock / with manufacturer's label certifying that both the container and the lock meet UL ratings).

Each office will be equipped with an approved firearms security container for temporary (on-duty) storage of handguns. This container is called a day safe and must be:

- Designed for the secure storage of a single handgun (one handgun per compartment if a multiple unit);
- Equipped with a key or combination lock;
- Mounted securely to a wall or office desk without exposed bolts or screws; and
- Devoid of any markings or lettering to indicate that firearms are stored inside.

The NFC maintains a list of approved security containers. Combination locks to firearms safes and designated firearms storage areas will be changed during the following conditions:

- When the safe or lock is originally received;
- When an employee who knows the combination retires, terminates employment, or transfers to another office;
- Whenever the combination is compromised; or
- Once every three calendar years.

130.15.3.1 Firearms Log. Each division has individually assigned firearms (*e.g.*, handguns) and unassigned firearms (*e.g.*, shotguns, rifles) stored in gun safes. The placement into storage and the subsequent removal from storage of any firearm from a gun safe will be documented on TIGTA OI Form 6600, *TIGTA Firearms Log*, by the individual who removes or replaces the firearm. Each FI or DFC will ensure that a hard copy of this log is maintained in, or with, the gun safe to document removal and return of the firearm.

130.15.4 Firearms Security in Motor Vehicles. Motor vehicles are not suitable for storing firearms. Never leave a firearm in a motor vehicle overnight. SAs will ensure that:

- Firearms are not stored in an unattended motor vehicle for longer than necessary;
- Firearms are not visible to passers-by;

- Firearms are placed in the most secure area of a motor vehicle (*e.g.*, the trunk if a vehicle is so constructed or a vault designed to be secured in and to a vehicle); and
- All vehicle doors and windows are locked.

Avoid removing or storing firearms and/or related equipment in a motor vehicle when these actions could be visible to passers-by.

130.15.5 Reporting Lost or Stolen Firearms. All SAs must notify their immediate supervisor immediately when a firearm is lost or stolen. The SA must also notify the appropriate local law enforcement authority and obtain a copy of the report of the stolen firearm. See Chapter 600, Section 130 for additional reporting requirements.

The SAC must report any loss of a firearm to the DAIGI, the appropriate AIGI and the NFC and ensure that a report of the lost or stolen firearm is entered into National Crime Information Center as soon as possible.

130.16 Ammunition.
Use only newly manufactured ammunition purchased by TIGTA in issued firearms. Do not use reloaded ammunition. The NFC purchases all TIGTA ammunition. Ammunition specifications are posted on TFSD's intranet site.

SAs must qualify with standard duty ammunition unless the range being utilized requires the use of "clean/green" ammunition. SAs should replace the duty ammunition every six months with fresh ammunition. "Clean/green" ammunition will not be used for duty carry.

130.16.1 Non-Duty Ammunition. Contact the NFC if the following types of ammunition are needed for training:

- Use .40 S&W training ammunition, 125 grain frangible non-toxic lead free bullet if the range requires lead-free (clean/green) ammunition, if the SA requires lead-free ammunition for health reasons (*e.g.*, pregnancy), or if the range requires frangible ammunition (*i.e.*, for use with steel targets);
- Use NLTA if the training involves use of modified firearms for NLTA; and
- Use birdshot for shotgun training where required.

130.16.2 Non-Lethal Training Ammunition. FLETC defines training non-ammunition that fires a marking cartridge during live target or force-on-force training as NLTA. Only use NLTA in firearms modified for non-lethal training. Contact the NFC for approval to use NLTA and equipment and to arrange for its shipment prior to scheduling such training.

Non-lethal training ammunition has been, and can be, involved in deadly training accidents. Extreme safety protocols and procedures must be exercised when conducting training that utilizes NLTA.

130.16.3 Ammunition Inventory Control. Each DFC, except for the Headquarters DFC, is responsible for reporting to the SAC the division's ammunition on hand as of September 30th of each year. The NFC will report this information for the Headquarters DFC on the TIGTA Ammunition Inventory Record (See the TFSD's intranet site).

The DFC will record all transfers of ammunition to FIs on the ammunition log. The FIs will document receipt and usage of all ammunition transferred to them. FIs will update the TIGTA Ammunition Inventory Record after each quarterly qualification/training cycle and forward to the DFC along with training records for that qualification.

The NFC will query the DFCs concerning their ammunition inventory as part of the annual budget process. The NFC will request and procure sufficient ammunition for the coming fiscal year. This process takes into account each division's requirements for duty, qualification, and training ammunition. Inventory planning should consider ammunition needs for 18 months.

When the DFC receives a shipment of ammunition:

- Confirm that it is the correct type of ammunition;
- Check for damage to shipping containers, and if practical, complete a random check of the ammunition to confirm its serviceability;
- Inventory the shipment;
- Mark the date of receipt on the case;
- Notify the NFC of receipt within three duty days;
- Add to the divisional inventory; and
- Store the ammunition properly.

130.16.4 Ammunition Storage. Store ammunition in a secure room or locked in a security container. Store ammunition in a cool, dry environment. Use older ammunition first to prevent inventory aging. Store dummy ammunition separately.

130.16.5 Ammunition Disposal. Contact the NFC for instructions on disposal of unserviceable ammunition.

130.16.6 Fired Cartridge Cases. Fired cartridge cases (brass) must be disposed of as follows:

- If the host agency will accept the fired cartridges (brass) at no charge to the Government, collect and leave at the range; and

- If host agency will not accept, follow GSA regulations for collection and transfer to GSA for disposal.

130.17 Firearms Maintenance.
Each SAC will ensure that firearms within their division are properly maintained by a factory trained/certified armorer. DFCs and armorers must maintain certification for one or more of the TIGTA-owned or issued firearms.

130.17.1 Armorers. The SAC should select armorers in consultation with the DFC to ensure adequate firearms maintenance throughout the division. Armorers should be selected based upon demonstrated interest, skill, and aptitude for firearms maintenance. Divisions may have more than one trained armorer. Armorers are not required to be certified on all three types of firearms; however, SAs who receive armorer training should be active participants in the division's firearms program.

Factory trained/certified armorers maintain specialized tools for the maintenance of firearms. Armorers should coordinate through their respective DFC to purchase their inventory of these specialized tools.

130.17.2 Firearms Malfunctions. All firearms malfunctions must be reported immediately to an FI, armorer, or the DFC. Once a malfunction has occurred, the firearm must be taken out of service until the problem is corrected and the firearm tested. When malfunctions occur during training every effort should be made to resolve the problem prior to leaving the range. The cause and resolution of all firearms malfunctions must be documented by the FI, armorer, or DFC as follows:

- Shooter error will be documented in a memorandum and maintained in the SA's officer safety training file;
- Firearm-related problems will be documented on the firearm maintenance log; and
- Ammunition failures will be reported by memorandum to the DFC and NFC.

130.17.3 Cleaning. All firearms must be cleaned within one day of firing. During the cleaning process, the user must inspect the firearm for defects and report any exceptions to an FI, armorer, or the DFC. If an armorer cannot repair the firearm, it will be returned to the factory for service.

Extreme weather conditions, moisture, and other environmental factors can contribute to firearms malfunctions. SAs must routinely inspect, clean, and lubricate firearms to ensure reliability. The same level of care should be taken with respect to ammunition and accessories.

130.17.4 Required Maintenance. Each firearm will be detail-stripped by a factory certified armorer once every three years. Parts will be replaced as needed, or as

recommended, by the manufacturer. The armorer must replace any defective, broken, or damaged parts. Replace any parts not within factory or TIGTA specifications.

Inspections must be documented in PPM in the Firearms Work Orders Section (FWOS). Document parts replacement and other maintenance performed in the PPM FWOS. In addition, the DFC/armorer should discuss usage with the assigned SA and enter an estimate of the rounds fired in the log.

SAs will inspect their magazine floor plates regularly for signs of excessive wear or fatigue. Damaged or cracked magazines will be taken out of service.

Each TIGTA firearm must be test-fired before duty use if:

- Any part is replaced, other than magazine floor plates; or
- Any action other than a normal breakdown for inspection, cleaning, and lubrication is taken.

130.17.5 Individuals Authorized to Perform Firearms Maintenance. Except as authorized below, SAs will not perform maintenance on any firearm beyond simple fieldstripping, cleaning, and lubrication. SAs with current armor training certification from the firearm's manufacturer are authorized to detail strip the firearm, replace parts (*e.g.*, sights, grips, recoil springs), and assess serviceability. The original manufacturer of the firearm, or a repair facility recognized as acceptable by the manufacturer, are the only authorized facilities to make repairs.

130.17.6 Functioning Standards and Modifications of Firearms. Firearms will always meet the manufacturer's standards for safe and reliable functioning. Unless specifically authorized by the NFC and approved by the DIGI, use only parts made by the original firearms manufacturer. An armorer must inspect and test fire a firearm before it is issued to an SA for duty use.

Any modifications to TIGTA-owned firearms must be approved by the NFC. Coordinate disposal of firearms, which are no longer functional and too costly to repair, with the NFC. See Section 130.19.

130.17.6.1 Functioning Standards of Personally-Owned Handguns. An FI/DFC will initially inspect all approved personally-owned handguns before the handgun may be fired during firearms qualification or alternate holster familiarization.

130.17.7 Firearms Maintenance Records. DFCs will document all firearms maintenance (other than routine cleaning) and repair in the PPM FWOS. Firearms maintenance records are not needed for permanently deactivated training firearms. If a firearm is transferred, a printed copy of the maintenance log must be forwarded to the gaining office.

130.18 Inventory Control.
PPM is the only authorized inventory system for tracking TIGTA firearms and body armor. All TIGTA firearms and body armor will be listed in the PPM inventory. Include temporarily or permanently deactivated training firearms. Inventories are maintained in PPM by the NFC and DFCs. The TIGTA Property Manager is the only individual who may delete items.

130.18.1 Annual Inventory Reconciliation. The DFC must submit an annual reconciliation of firearms and body armor on-hand in their division by January 31 of each year. This reconciliation is submitted through the SAC to the DIGI with a copy provided to the NFC. This report will account for the following:

- All officer safety equipment on hand, issued and, unassigned;
- All firearms on hand, issued and unassigned; and
- All body armor on hand, issued, and unassigned.

In the course of this reconciliation process, the DFC directs an individual inventory of each SA's issued officer safety equipment. This equipment will be examined for operational readiness. Unserviceable equipment will be identified and replaced. Damaged and/or missing equipment will be reported to the SA’s supervisor for appropriate action.

The DFC maintains physical custody of all unassigned firearms and unassigned body armor in the Division.

130.18.2 Accounting for Firearms/Officer Safety Equipment. Prior to separation from TIGTA, the SA must return their assigned handgun, body armor, and all other officer safety equipment to the local FI or ASAC prior to their departure. The DFC ensures that this equipment is serviceable before reissuing it and takes appropriate action if it is not serviceable. The DFC will maintain unassigned body armor for the use of armed escorts.

130.18.3 Transfer of Firearms/Officer Safety Equipment. DFCs are responsible for preparing Form OI 1931, *Transfer Receipt of Personal Property*, when firearms, body armor, or officer safety equipment are transferred to another division. The DFC of the division receiving such transferred firearms/officer safety equipment must complete, sign, and return Form OI 1931 to the originating DFC within two working days to acknowledge receipt of the items. A copy of this Form OI 1931 will be sent to the NFC via the TFSD Inbox (*TIGTA Inv TFSD) so that the PPM database can be changed to reflect the transfer.

130.18.4 Transfer of Officer Safety Equipment and Equipment Assigned to an SA.
When officer safety equipment transfers between divisions, the DFC will use a Form OI

1931. When an SA transfers between divisions, the losing office DFC sends the appropriate custody receipts for these items to the gaining office DFC.

130.19 Destruction of Firearms.
The NFC is the only person authorized to dispose of firearms. When a TIGTA firearm is not required by a division, the DFC will contact the NFC for disposal instructions.

The NFC determines whether the firearm is serviceable for other law enforcement use or is unique to be of interest to a Federal museum.

130.20 Shipment of Firearms.
All firearms will be shipped via traceable overnight mail. If traceable overnight mail is not available, contact the NFC to determine an acceptable alternative. The individual shipping the firearm must:

- Pack the unloaded firearm in a locked shipping container with appropriate padding (lockable hard shell container);
- Use appropriate number and types of locks;
- Enclose a Form OI 1931 including the names, addresses, and telephone numbers of both the shipping and receiving individuals;
- Notify the recipient and verify the address and telephone number;
- Record and retain tracking number for shipments in transit; and
- Verify that the firearm was received. Initiate immediate action to locate an undelivered firearm. If the firearm cannot be located, advise the DFC, SAC, and NFC immediately.

Do not ship firearms on Friday, or the day before a Federal holiday unless it is required to meet operational needs. Notify the NFC of such shipments.

130.21 Shipment of Hazardous Materials.
Hazardous materials such as ammunition, OC spray, lithium batteries, etc. will be shipped in accordance with Title 49, Subtitle B, Chapter I, Subchapter A of the United States Code of Federal Regulations. DFCs and employees handling hazmat materials will meet all Department of Transportation Hazardous Material Regulations.

DATE: July 1, 2020

CHAPTER 400 – INVESTIGATIONS

(400)-140 Field Operations and Enforcement Activities

140.1 Overview.
This Section pertains to the Office of Investigations' (OI) field operations and enforcement activities, including:

- Authority
- Classification of Investigative Operations
- Arrests
- Arrest Warrants
- Summons
- Wanted Posters
- Search Warrants
- Warrantless Searches
- Inventory of Seized Property
- Physical Surveillance

140.1.1 Acronyms Table.

140.2 Authority.
The Inspector General Act of 1978, as amended, authorizes special agents (SA) to make arrests, with or without a warrant, to execute search warrants, to serve subpoenas and summonses, and to make seizures of personal property subject to the Internal Revenue laws in accordance with the provisions of Title 26, U.S.C. § 7608(b). See Section 10.

140.3 Classification of Investigative Operations.
Investigative operations are classified as field operations, special operations, and undercover (UC) operations. See Section 180 for special operations and UC operations.

140.3.1 Field Operations. Field operations include the following:

- Execution of arrest warrants;
- Execution of search warrants;
- Armed escorts;
- Multi-agent surveillance; and
- Other operations that do not involve militant, anti-government or other known organized criminal groups or gangs. See Section 180.3.

The Special Agent in Charge (SAC) is the approving official for all field operations. However, the respective Deputy Assistant Inspector General for Investigations (DAIGI) and/or Assistant Inspector General for Investigations (AIGI) must be notified immediately upon the completion of all field operations involving the execution of an arrest or search warrant.

140.3.2 Operational Planning of Field Operations. An approved operational plan should be in place prior to the initiation of all field operations if Treasury Inspector General for Tax Administration (TIGTA) is the lead investigative agency. For field operations where TIGTA is not the lead investigative agency, no TIGTA operational plan is required, provided the lead investigative agency has a documented operational plan. See Section 140.8.2.

TIGTA SAs should obtain a copy of the lead agency's operational plan and maintain it in the TIGTA case file. If the lead investigative agency has no documented operational plan, the TIGTA SA should, as circumstances dictate, prepare and obtain approval of a TIGTA operational plan prior to the initiation of the field operation. See Section 140.8.2.

There are two types of operational plans:

- TIGTA Form OI 7503, *Operational Plan for Search Warrant*; and
- TIGTA Form OI 7504, *Operational Plan for Armed Escort, Surveillance, Undercover, and Arrest*.

140.3.3 Transmitting Information. All field operations information should be considered law enforcement sensitive and protected from unauthorized disclosure. Information transmitted electronically should be sent by encrypted e-mail. When transmitting hard copies, place the information in a security envelope labeled, "To Be Opened by Addressee Only," seal the security envelope with tape, and place it in the shipping envelope. The entire shipping address should be placed on both envelopes. If the information is received in either a torn or opened security envelope, establish if the contents may have been compromised and notify the case agent's Assistant Special Agent in Charge (ASAC) and SAC for appropriate action.

140.4 Arrests.
A TIGTA SA may execute an arrest based on statutory or non-statutory authority.

140.4.1 Statutory Arrest Authority. SAs derive their arrest authority from the Inspector General Act of 1978, and Treasury Order 115-01, and Title 26 U.S.C. § 7608(b)(2).

140.4.2 Non-Statutory Arrest Authority. The primary responsibility of a TIGTA SA is conducting official investigations of offenses arising from the administration or enforcement of laws relating to the Internal Revenue Service (IRS). However, in the

absence of a controlling Federal statute, the laws of arrest in the State where the arrest is made is controlling.

In addition, SAs may have State peace officer arrest authority. It is important to know the law of the particular State in which the SA is located to determine whether State peace officer status exists and whether citizen's arrest or detention authority exists. See Section 20.10, for more information concerning peace officer status.

140.4.3 Warrantless Arrests. An arrest without a warrant is a serious matter, and it could subject the person making the arrest to civil and/or criminal liability. False imprisonment, false arrest, or other action could result in administrative review.

For SAs acting as private citizens to be privileged to make a warrantless arrest, it is generally necessary that a violation constituting a felony be committed in their presence, or that the SAs have reasonable grounds to believe the person they arrest has committed a felony. See Section 20.10, for more information concerning peace officer status.

140.4.3.1 False Arrest. An arresting SA may incur liability for monetary damages in a tort action for false arrest, false imprisonment, or assault and battery, depending on the circumstances surrounding the false arrest.

140.5 Arrest Warrants.
An arrest warrant is signed by a Federal magistrate and contains the name of the defendant or description by which the defendant can be identified with reasonable certainty. It also contains a description of the offense charged in the complaint and commands that the defendant be arrested and brought before the nearest available magistrate.

140.5.1 Probable Cause. Probable cause is defined as a set of facts or apparent facts, which are sufficiently strong in themselves to lead a reasonable, prudent law enforcement officer to believe that the person to be arrested committed the offense charged. Probable cause, based upon oath or affirmation, must be met in the warrant of arrest.

When applying for an arrest warrant where there is probable cause to believe that evidence of a crime can be found at a specific location, contemporaneously apply for a search warrant. See Section 140.8.

If probable cause is developed after the arrest, then apply for a search warrant in a reasonable amount of time while members of the arrest team remain on the premises to prevent destruction of evidence. Options for securing such a warrant include, but are not limited to, telephonic or electronic communications. See Section 140.8.

140.5.2 Execution and Return of Arrest Warrant.
Upon arrest, the SA possessing the original or a duplicate original warrant must show it to the defendant. If the SA does not possess the warrant, the SA must inform the defendant of the warrant's existence and of the offense charged and, at the defendant's request, must show the original or a duplicate original warrant to the defendant as soon as possible.

The arrest warrant can be executed at any place within the jurisdiction of the U.S.

SAs should make every effort to execute their own arrest warrants. The SA who executed the arrest warrant must return it to the issuing district as soon as practical.

140.5.3 Planning the Arrest. Prior to executing an arrest warrant, SAs must prepare TIGTA Form OI 7504. SAs must obtain approval for the plan from the SAC unless, in rare instances, exigencies preclude a written plan. It is the responsibility of all SAs to ensure there is an effective operational plan in place.

140.5.4 Executing the Arrest. Plan the arrest to minimize opportunities for the subject to either resist or flee. When making an arrest, SAs should, at a minimum, follow the below procedures:

- Arresting SAs must promptly identify themselves as Federal law enforcement officers and clearly advise the subject that he/she is under arrest;
- Use only reasonable and necessary force but do not hesitate to use such force as necessary to effectively and expeditiously bring under control a person who initiates action to cause physical harm;
- Inventory the subject's personal property;
- After arresting, handcuffing, and searching the subject, transport the subject to a predetermined site for processing; and
- Apprise the subject of his/her rights as afforded under the *Miranda* decision.

140.5.4.1 Entry of Residence When Making Arrest. SAs are not authorized to enter a suspect's home to make an arrest unless an arrest warrant has been issued. Exceptions to this rule are “hot pursuit” and exigent circumstances. Enter a suspect's home to effect an arrest only if there is reasonable belief that the suspect is present. Prior to entry give, or make a reasonable effort to give, notice and purpose for entry unless otherwise justified by exigent circumstances.

Do not enter the residence of a third party not named in the arrest warrant without one of these circumstances present:

- Third-party's consent;
- "Hot pursuit;”

- Search warrant; or
- Exigent circumstances.

140.5.5 Arrest Precautions. In accordance with the Treasury Department's Policy on the Use of Force (See Treasury Order 105-12), SAs may use a reasonable level of force necessary to effect an arrest. SAs may also establish liaison and seek assistance from local law enforcement agencies in potentially dangerous arrest situations. See Section 120.3 of this chapter for information related to TIGTA's Use of Force Policy.

To accomplish the safe delivery of arrestees, SAs must handcuff every arrestee with their hands behind their back, unless the arrestee has a physical handicap or health problem that would make handcuffing in this manner impractical or unsafe. SAs must:

- Resolve any doubt in favor of using handcuffs and other restraining devices;
- Maintain a close guard over an arrestee at all times, as handcuffs are only temporary controls;
- When an arrestee is cuffed with hands in front, use belly chains or other appropriate device to hold their cuffed hands to their body to prevent them from using the cuffs as a weapon; and
- Never handcuff an arrestee to a fixed object inside a vehicle.

140.5.6 Use of Firearms During Arrest. The Treasury Department's Policy on the Use of Force (See Treasury Order 105-12) and TIGTA's Use of Force Policy should be followed at all times. See Section 120.3 of this chapter for information related to TIGTA's Use of Force Policy.

Promptly notify the appropriate AIGI in all cases in which a subject, an SA, or an accompanying police officer discharges their firearm. See Section 120 of this chapter for additional information on procedures following use of force incidents.

140.5.7 Reporting Arrests. Notify the appropriate DAIGI and/or AIGI through your management chain, whenever an arrest is made. If the arrestee is an IRS employee, also notify the appropriate DAIGI and/or AIGI prior to making the arrest.

140.5.8 TECS/National Crime Information Center. The SA obtaining the arrest warrant must ensure that the warrant is entered into TECS/National Crime Information Center within 24 hours of obtaining the warrant. See Section 150, for warrant entry procedures.

140.5.9 Transporting Prisoners. If transporting a prisoner over a long distance or for a long duration of time, the SA should consider the following:

- Suitable prisoner transport belts of leather, fabric, or chain, with or without integral handcuffs, may be attached around a prisoner's waist to restrain movement;
- Suitable devices of leather, fabric, or chain may be used to encircle a prisoner's ankles or legs to further restrain the prisoner's leg movement; and
- Use of transport belts requires increased monitoring of prisoners due to front placement of the prisoner's hands.

TIGTA vehicles utilized in arrest operations shall be searched prior to the operation to ensure no contraband exists in the vehicle. Prisoners transported in TIGTA vehicles must be thoroughly searched prior to being placed in the vehicle. All prisoners transported by automobile will be secured in the vehicle with a seat belt.

See Section 130.11.2 for types of restraining devices.

140.5.10 Fingerprinting, Booking, and Deoxyribonucleic Acid Sampling. After the arrestee is taken into custody, the SA will transport the arrestee to the U.S. Marshals Service (USMS) for processing, or "booking." SAs will obtain and transmit fingerprints from the arrestee at the time of booking using an electronic fingerprinting system and will coordinate with the booking agency to input the biographical, arrest, and other relevant data associated with the arrestee.

TIGTA's unique Originating Agency Identifier (ORI) DCTIX0000 shall be entered into the USMS Joint Automated Booking System (JABS) at the time of booking.

Note: TIGTA's ORI can be found in JABS by:

- Selecting Department of Treasury and Finance (DTF) in the agency tab;
- Selecting DC in the State tab; and
- Selecting TIGTA or DCTIX0000 in the ORI tab.

SAs will obtain a Deoxyribonucleic Acid (DNA) sample from an arrestee at the time of booking using the Federal Bureau of Investigation's (FBI) Buccal Collection Kit and will forward the sample to the FBI at:

FBI Laboratory
Attn: Federal DNA Database Unit
2501 Investigation Parkway
Quantico, VA 22134-9902

Instructions regarding the collection of a DNA sample can be found on the FBI's website.

140.5.11 Arresting Foreign Nationals. Treaty obligations of the U.S. require that certain procedures be followed when arresting a foreign national. These procedures are in addition to any other rights or privileges afforded to individuals under arrest. Refer to the State Department's Consular Notification and Access Manual, for additional information.

Whenever a foreign national is arrested, notify the appropriate DAIGI and/or AIGI through your management chain.

140.5.11.1 Additional Rights Advisement. Advise a foreign national of the right to have his/her government informed of the arrest. Notify the appropriate foreign consulate or embassy without delay, if the arrestee wishes to exercise this right. Document this advisement in the TIGTA Form OI 2028-M, *Memorandum of Interview or Activity,* noting the date and time of the advisement and the foreign national's requests, if any.

140.5.11.2 Consulate or Embassy Contact. Bilateral agreements between the U.S. and certain countries require notification of a consulate or embassy regardless of the arrestee's wishes. A list of these countries is outlined in the Consular Notification and Access Manual.

If notification to a consulate or embassy is requested or required, the SAC should conduct the necessary notification outlined in the Consular Notification and Access manual. This notification should be made within 72 hours. The SAC may delegate this authority to an ASAC, as appropriate. If contact is made via telephone, the SAC should prepare a written record of the conversation noting the date, time, person contacted, summary of conversation, and any consular requests. The written record can be made by the SAC completing a TIGTA Form OI 2028-M, or by annotating the TIGTA Form OI 6501, *Chronological Case Worksheet*. If the SAC elects to complete a TIGTA Form OI 2028-M, they should provide it to the case agent for inclusion into the investigative file.

140.5.11.3 State Department Contact. In the event the U.S. Department of State contacts TIGTA concerning the arrest, notification, or lack of notification, the Deputy Inspector General for Investigations (DIGI) or his/her designee will respond to the Department of State in accordance with disclosure laws.

140.6 Summons.
A summons contains the same elements as an arrest warrant, except that it commands the defendant to appear before a magistrate at a stated time and place. SAs should make every effort to serve their own summonses.

140.6.1 Service and Return of a Summons. A summons is served by delivering a copy to the defendant personally, or by leaving it with a responsible adult at the defendant's residence and mailing it to the defendant's last known address.

When serving a summons on an organization, deliver a copy to an officer, to a managing or general agent, or to another agent appointed or legally authorized to receive service of process. Also mail a copy to the organization's last known address within the district or to its principal place of business elsewhere in the U.S.

140.7 Wanted Posters. OI may issue a Wanted Poster for an OI arrest warrant for a fugitive whose whereabouts are unknown. If a violation of Title 26, U.S.C. is involved, consult with TIGTA's Office of Chief Counsel prior to requesting a Wanted Poster.

- Wanted Posters are mailed to Federal, State, and local law enforcement agencies; and
- Wanted Posters request that anyone with information concerning the subject contact the nearest TIGTA office listed on the back of the poster.

The SAC requests Wanted Posters by memorandum through the appropriate AIGI to the DIGI. The following information must be furnished:

- Case name and number;
- Justification for issuance of the poster;
- Full name of the subject;
- Photograph, if available;
- Fingerprints;
- Alleged criminal violation(s) as described on arrest warrant;
- Personal data including date and place of birth, weight, height, color of hair and eyes, occupation, and Social Security Number;
- Date of issuance of warrant and office or official holding warrant;
- Whether subject should be considered armed and dangerous;
- A copy of arrest warrant; and
- Any other pertinent data.

Upon approval of the request, the Operations Division will arrange, through the U.S. Department of the Treasury, the printing and mailing of the Wanted Posters to various Federal, State, and local agencies. A distribution list for each Wanted Poster issued is maintained by the SAC of the issuing division.

When the subject of a Wanted Poster is either apprehended, or the poster's need is withdrawn, advise the DIGI, through the appropriate AIGI, by memorandum, as soon as possible. A cancellation notice will then be sent to all recipients of the Wanted Poster.

140.8 Search Warrants. The SA will adhere to all commanded items of the signed search warrant obtained.

Section 41(d)(2)(A) of the Federal Rules of Criminal Procedure provides that Federal search warrants may be requested by a Federal law enforcement officer, and issued by a Federal judge or State court approving the search of a property and people.

140.8.1 Operational Plan for Search Warrant. An approved operational plan must be in place prior to the initiation of a search warrant if TIGTA is the lead investigative agency, unless approved by the SAs supervisor. TIGTA Form OI 7503, *Operational Plan for Search Warrants* will be used to document personnel assignments, purpose and targets of the activity, equipment identification, and emergency procedures related to the search warrant.

140.8.2. Other Agency is the Lead Investigative Agency. For search warrants where TIGTA is not the lead investigative agency, no TIGTA operational plan is required, provided the lead investigative agency has a documented operational plan. TIGTA SAs must obtain a copy of the lead agency's operational plan and maintain it in the TIGTA case file.

140.8.3 Search Warrants Obtained Pursuant to 18 U.S.C. § 2703. Unlike traditional search warrants, 18 U.S.C. § 2703, *Required Disclosure of Customer Communications or Records*, does not require a sworn law enforcement officer to be present onsite during the execution of the warrant. When a Federal warrant is obtained under 18 U.S.C. §2703, an approved operational plan is not required to be completed prior to the execution of such a warrant.

140.8.4 Search Warrants for U.S. Mail. If a Federal search warrant is executed on a United States Postal Service facility to seize such mail, an approved operational plan is not required to be completed prior to the execution of such a warrant.

140.8.5 Execution of Search Warrant. A physical search warrant shall be served in the daytime unless the court provides in the warrant and for reasonable cause shown that it may be served at times other than daytime. The term "daytime" means the hours between 6:00 a.m. and 10:00 p.m., according to local time. The warrant must be executed and a return made to the magistrate or judge within the period specified in the warrant, not to exceed 14 days from the date of the warrant.

140.8.6 Return of Search Warrant With Inventory. If no one is present during the search, a copy of the search warrant must be left in a conspicuous place so that the owner of the premises may find it. If no property is seized, the SA is only required to leave a copy of the warrant with the person or at the premises searched.

When taking property pursuant to the authority of the search warrant, list the property on the inventory found on the reverse side of the search warrant or use an attachment as needed. The list must be made in the presence of another officer and the person from whose premises the property was taken if that person is present and available. If either another officer or the person from whose premises the property was taken is not present, the inventory must be made in the presence of a least one credible witness.

All property taken from the premises during the execution of a search warrant must be accounted for. Items not related to the search, but seized under plain view, must be accounted for on a separate receipt. No specific form or format exists for this separate receipt. The SA should put the information as required by the nature of the seized item on a plain sheet of paper and leave it either with the person whose premises have been searched or on the premises itself. If permitted under 26 U.S.C. § 6103, notify the appropriate law enforcement agency about the "plain view" items seized. Although a prompt return is required by the rule, a failure to make a prompt return will not invalidate the search warrant or the items seized, since this is held to be only an administrative procedure after the search.

140.8.7 Digital Evidence Search Warrant Considerations. SAs will consult with the Digital Forensic Support (DFS) Group when preparing applications for the issuance of search warrants, if the property being searched or seized involves computers, mobile phones, or other information stored in digital form. The Cybercrime Investigations Division (CCID) will follow divisional guidelines and generally only contact DFS on an as-needed basis.

140.9 Warrantless Searches.
There are situations in which SAs are permitted to search without a warrant, including but not limited to, 1) searches incident to an arrest; and 2) searches made with consent.

140.9.1 Searches Incident to Lawful Arrest Without a Search Warrant. Incident to any lawful arrest, a SA may contemporaneously search both the arrestee's person and the area within the immediate control of the arrestee including vehicles, into which that person might reach to obtain weapons, means of escape, and any evidence to prevent it from being concealed or destroyed. Once the arrestee has been removed from the scene of the arrest, SAs may not go back to where the arrest took place to search because the arrest, thus the exigency of the moment, has passed and the search would not be "contemporaneous."

Whenever possible, a SA of the same sex should search the arrestee.

In addition, other limited searches incident to arrest defined as protective sweeps are acceptable, which are conducted to protect the safety of SAs and others.

140.9.2 Searches Made with Consent. An SA may conduct a search without a warrant with the voluntary consent of the person who has apparent authority to give the consent. Any coercion or deception will invalidate the consent for the search.

Whenever possible, obtain a written waiver of Fourth Amendment rights from the person granting consent. See TIGTA Form OI 1934, *Written Consent to Conduct Search*, for format of written waiver. In situations where consent is given to search remote digital accounts (*e.g.*, social media, e-mail accounts) TIGTA Form OI 1935, *Written Consent to Conduct Search – Digital Device/Storage/Account*, should be used. The recommendation is to consult with DFS prior to the issuance of Form OI 1935. CCID may utilize additional consent forms or contact DFS, as appropriate.
Consent may be withdrawn during the course of the search, at which time the search must be stopped. Consider application for a search warrant. Anything seized before revocation of the consent may be introduced into evidence or used as probable cause to obtain a warrant.

140.10 Inventory of Seized Property.
Secure any property in the physical control of arrestees or seized as evidence or forfeiture. Inventory all vehicles and other property that are taken into custody.

See Section 190 of this chapter for the policy pertaining to evidence handling and safeguards.

140.10.1 Inventory Procedures. Limit the inventory to locating valuables or harmful items for secure storage. An inventory is not a search for evidence. Advise the subject of the purpose of the inventory and results of the inventory at the time of arrest or as soon after the inventory as practical.

- Conduct the inventory at the time of the arrest, or as soon as practical after the arrest;
- Conduct a detailed inventory of all property, including the contents of containers and vehicles in the custody and control of the Government; and
- Open all compartments, including locked or closed containers, and catalog all items found.

Prepare TIGTA Form OI 2028-M or inventory listing showing the results of the inventory.

Include the following documentation when making an inventory of vehicles:

- Year, make, model, color, vehicle identification number, license number;
- Name and identifying information of the vehicle operator and the owner, if different from the operator;
- Description of all valuables secured from the vehicle;
- List of all accessories, tools, and unattached parts left in the vehicle;

- Description of the condition of the body and upholstery (list damaged or deteriorated areas, stating extent of damage); and
- List of all missing items such as keys, motor, radio, battery, or spare tire.

All property that constitutes contraband or evidence of a crime is subject to seizure. If permitted by 26 U.S.C. § 6103, notify the appropriate local or State agency if property seized is not evidence of a Federal crime.

140.10.2 Property Held for Security Purposes. Secure cash, credit cards, jewelry, furs, weapons, electronics, etc., in evidence lockers, locked cabinets, or other facilities under the control of the Government. Limit access to these facilities to the seizing SA and the evidence custodian.

140.10.3 Seized Vehicles. Impound and store vehicles at a secure location or a facility used by other Federal, State or local law enforcement agencies.

- Contact the USMS to arrange for storage if no other adequate facilities are available; and
- Adhere to impound procedures of the agency providing storage.

Prior to seizing a vehicle, the SA shall take photographs of all angles of the vehicle. Document the overall condition of the vehicle and photographs on Form OI 2028-M.

140.10.4 Inventory Listing. Place the original Form OI 2028-M and/or the inventory listing in the investigative case file. Leave a copy with or attached to the property. Give a copy of the listing to the storage facility representative, and a copy to the person from whom the property was seized. If the owner of a seized vehicle is not the operator/arrestee, mail a copy to the owner at the address of record on the vehicle registration.

140.10.5 Release of Property. Secure all property until it is properly disposed of or released to the owner or person from whom it was seized. Do not release any property until the owner provides a completed release/receipt to the releasing SA.

140.11 Physical Surveillance.
Whenever possible agents should conduct physical surveillance with another law enforcement officer. If agents are conducting surveillance by themselves, SAs must notify their ASAC of their location, start time, end time, and provide regular status notifications. SAs may also notify local law enforcement of their intent to conduct surveillance and for de-confliction.

140.11.1 Approval to Conduct Surveillance. SAs must notify their supervisor prior to conducting non-large-scale surveillance activities unless exigent circumstances require conducting an immediate surveillance. SAs must obtain supervisory approval for large scale and/or multiday surveillance.

ASACs are authorized to approve surveillance, except in the following circumstances:

- Surveillance activity constituting a special operation or an UC operation as defined in Section 180 of this Chapter;
- High-risk, or extremely sensitive circumstances;
- Surveillance activity conducted for the purpose of gathering national security intelligence; and
- The use of TIGTA SAs outside the ASAC's group.

The circumstances outlined above require approval by a SAC or higher-level management official, and completion of TIGTA Form OI 7504 is required.

140.11.2 Surveillance Involving Multiple Special Agents. For all surveillance activities involving more than three agents, an operational plan or operational briefing will be used to ensure safe and efficient coordination of each participant's activities. When participants of a surveillance activity are from geographic locations outside the area in which the surveillance activity will be conducted, the case agent must ensure that all participating agents are briefed on the details of the operation and that such briefings are documented in TIGTA Form OI 6501.

These briefings must include the following information, as appropriate:

- Information about the subject(s) of the surveillance (*e.g.*, name, physical description, criminal history);
- The location of the surveillance (if mobile surveillance, identify likely locations);
- Names and assignments of all participating special agents;
- Information relating to communication among the participating agents (*e.g.*, cell phone numbers, radio frequencies);
- Names and contact numbers of the cognizant Assistant United States Attorney and local police, if applicable;
- The location of local police stations in the immediate area;
- The location of hospitals/medical facilities in the immediate area; and
- Any other information that would substantially contribute to a safe and effective surveillance activity.

The SA will prepare and obtain approval of TIGTA Form OI 7504 prior to initiation of surveillance activities involving more than three TIGTA SAs, unless exigent

circumstances require that an immediate surveillance be conducted or TIGTA is not the lead agency.

140.11.3 Restrictions During Surveillance. SAs are responsible for knowing and obeying local speed limits and traffic laws during surveillance activities. In rare instances, pursuit or emergency response driving may be justified during surveillance. See Section 110 of this Chapter for detailed information.

DATE: April 1, 2021

CHAPTER 400 - INVESTIGATIONS

(400)-150 Investigative Sources of Information

150.1 Overview.
This Section contains information regarding investigative sources of information:

- Authority
- Confidential Sources
- Law Enforcement Databases
- Mail Covers
- Taxpayer Data
- Centralized Authorization File
- Information from State or U.S. Territorial Taxing Authorities
- Social Security Administration Account Information
- Obtaining Wage and Other Income Statements
- Information Available Under the Bank Secrecy Act
- The National Instant Criminal Background Check System

150.1.1 Acronyms Table.

150.2 Authority.
Title 26, United States Code (U.S.C.) § 6103(h)(1) authorizes Treasury Inspector General for Tax Administration (TIGTA) employees to access tax returns and return information as long as the information is being sought in the performance of official tax administration duties (*e.g.*, Office of Investigations (OI) is conducting an investigation pursuant to the internal revenue laws [*i.e.*, Title 26] or related statutes). In non-tax administration investigations (*i.e.*, investigations not performed pursuant to the internal revenue laws or related statutes), TIGTA employees have limited authority to access tax returns and return information (*e.g.*, through the use of an ex parte order pursuant to 6103(i) issued to the Internal Revenue Service [IRS] or with taxpayer consent). See Section 70 and Chapter 700, Section 50 for a complete discussion of 26 U.S.C. § 6103 and the authority to access tax returns and return information.

Several of the sources of information listed in this section may consist of tax returns or return information protected by the confidentiality provisions of 26 U.S.C. § 6103.

150.3 Confidential Sources.
A confidential source (CS) is any person or entity that provides information or services on a confidential basis. The courts have recognized that the Government's use of a CS is lawful and often essential to the effectiveness of properly authorized law enforcement investigations.

Use of a CS to assist in the investigation of criminal activity may involve elements of deception, intrusion into the privacy of individuals, or cooperation with persons whose reliability and motivation can be open to question. OI may use a CS only in furtherance of its authorized investigative activities and law enforcement responsibilities. A CS cannot be directed to commit acts that OI would not authorize its own special agents (SA) to commit. A CS may be asked to:

- Provide information already in his or her possession or that comes to their attention;
- Affirmatively seek out information concerning misconduct, criminal conduct, or otherwise; or
- Provide operational assistance to OI.

SAs utilizing a CS should become thoroughly familiar with the Attorney General's Guidelines Regarding the Use of Confidential Informants (Revised May 30, 2002). When using a CS, the control agent should:

- Carefully evaluate and closely supervise the use of a CS;
- Ensure that individual rights are not infringed upon;
- Corroborate information by independent sources whenever possible;
- Debrief a CS as soon as possible after he/she obtains information relevant to a particular investigation or that is of interest to OI;
- Promptly analyze and document information; and
- Disseminate information of interest to another agency (unless prohibited by law or regulation and provided the safety of the individual or security of any investigation is not unreasonably compromised).

A CS is not an employee of OI. This should be fully explained to the CS and is further addressed in TIGTA Form OI 9834, *Instructions to Confidential Source*. The CS's relationship to OI can impose a special responsibility upon this agency when the CS engages in activity where they have received, or reasonably think they have received, encouragement or direction for that activity from OI.

150.3.1 One-Time Sources. Individuals who furnish information on a one-time basis and request confidentiality should be processed as follows:

- Refer to a one-time source in all TIGTA OI forms by a temporary identifier ("T-1," "T-2,") etc.;
- Refer to a one-time source in TIGTA's Criminal Results Management System (CRIMES) by a temporary identifier ("T-1," "T-2," etc.); and
- Documentation of a one-time source's true name, address, Social Security Number (SSN), occupation, and associated documents related to the source shall be maintained in a folder titled "Restricted File" that is associated with the

appropriate Intake or Investigation in CRIMES. In order to create the "Restricted File" the case agent must enter a specialized technique in CRIMES, which provides the agent with the ability to control access. See CRIMES User Manual.

See Section 180 regarding procedures related to Undercover Identities.

See Section 210 regarding procedures for granting a pledge of confidentiality to IRS employees who furnish information about the subject of an investigation.

The Special Agent in Charge (SAC) has authority to designate one-time sources.

If a third party references the name of an individual in a separate interview, who has previously been designated as a one-time source, use the individual's name as opposed to the temporary identifier ("T-1, T-2," etc.) should be used.

150.3.2 Confidential Source. A CS is any person or entity, providing information or services on a confidential basis, whether compensated or not. The information obtained by the CS may be the result of an association with a person of investigative interest, and whose identity, if generally known, would impair the relationship between the CS and OI, or could cause physical, emotional, or economic harm to the CS. The furnishing of such information or services by a CS:

- May be the result of legitimate employment endeavors, or access to records;
- Must be consistent with OI rules and regulations and in compliance with applicable law; and
- May be the result of association with persons of investigative interest (*e.g.*, a person who is the subject or who may be reasonably expected to become the subject of an investigation).

Consult with the United States Attorney's Office (USAO) prior to using a CS to contact a subject who is represented by an attorney.

A CS who provides information on a continuing basis will not be authorized to participate in activities that would otherwise be criminal, nor be used to provide substantial operational assistance in an undercover operation, unless an approving official has made a determination that:

- The CS appears suitable for such use; and
- The information likely to be obtained or the operational assistance to be provided is pertinent to authorized OI investigative activities or law enforcement responsibilities.

Complete a suitability evaluation for each proposed CS before making a decision to use the CS.

150.3.3 Documenting a Confidential Source. To initiate a request to designate a CS, contact the National Undercover Program Manager (NUPM). The NUPM will assign the prospective CS an identifier to be used in all reports and correspondence. The CS identifier will consist of the CRIMES division code for the originating division, followed by a three-digit sequential number.

150.3.3.1 Initial Record Checks. For each individual that is being considered as a CS, the following records will be reviewed:

- Police records (*e.g.,* criminal history, address and name checks);
- CRIMES indices;
- All OI reports concerning the proposed CS;
- Employee Official Personnel Folder, if applicable; and
- Federal Bureau of Investigation (FBI) name check.

The SA should ask the CS for consent to review the CS's tax information. If the CS agrees, have the CS complete the *Consent to Access Tax Returns and Return Information by the Treasury Inspector General for Tax Administration* form. See TIGTA Form OI 1933, *Consent for Release of Tax Return and/or Return Information by the Treasury Inspector General for Tax Administration.* See Chapter 700, Section 50 of the TIGTA Operations Manual for guidance concerning authority to access tax returns and/or return information.

The results of all record checks conducted related to the potential CS will be documented in TIGTA Form OI 9833, *Confidential Source Application*. If the potential CS has a criminal record, include a printout of the information and seal it in an envelope with a "Restricted File" label affixed and attach to the Confidential Source Application.

This review may only be used to assess CS suitability. It may not be used to develop information concerning an individual for the purpose of inducing or influencing him/her to become a CS.

150.3.3.2 Confidential Source Application. The control agent, who is typically the person who initially developed the CS, will complete TIGTA Form OI 9833, *Confidential Source Application*, to document a thorough description of the CS.

A copy of the CS file (*i.e.*, the CS application with attachments) will be forwarded to the NUPM for permanent retention. The NUPM is to be provided copies of all information and documentation included in the CS file retained by the field division.

150.3.3.3 Approval of CS Designation. Generally, the SAC has authority to approve the designation of a CS. Approval of CS designation by the Assistant Inspector General for Investigations (AIGI) or a Deputy Assistant Inspector General for Investigations (DAIGI) is required for a CS possessing a judicially recognized privilege of confidentiality, as indicated in Section 150.3.13.

To obtain approval of the CS designation, the SA will forward the CS application through their manager to the SAC (or DAIGI/AIGI if required) requesting the designation of a CS. The SAC will forward the CS application to the NUPM for review. Once the CS application is approved, the NUPM will return the approved CS application to the requesting SAC. The NUPM will then input the CS as a contact in CRIMES.

150.3.3.4 Suitability Factors. In determining the suitability of a CS, the approving official considers the following factors:

- Nature of the matter under investigation and the importance of the information or assistance being furnished;
- Seriousness of past and present criminal activity of which the CS may be suspected;
- Motivation of the CS, including any consideration sought from the Government for his/her cooperation;
- Likelihood that the information or assistance which a CS could provide is not available in a timely and effective manner;
- CS's reliability and truthfulness, or the availability of means to verify information which the CS provides;
- Any record of conformance by the CS to OI instructions and control in past operations and how closely OI will be able to monitor and control the CS's activities insofar as he/she is acting on behalf of OI;
- Any risk that the use of a CS may compromise an investigation or subsequent prosecution, including court-ordered disclosures of identity which may require the Government to move for dismissal of the criminal case; and
- Risk that use of a CS in the particular investigation may intrude upon privileged communications, or inhibit the lawful association of individuals or expression of ideas.

Consider administering a polygraph to a potential CS.

150.3.4 Restricted Types of Confidential Sources. Do not use the following persons as a CS without additional approval as specified below:

- Persons enrolled in the Witness Security Program may not be utilized without approval from the Department of Justice (DOJ);
- Federal probationers may not be utilized without approval of the U.S. Probation Office; and

- State parolees or probationers may not be utilized without prior notice to State officials.

150.3.5 Reviews of Suitability Determinations. The Assistant Special Agent in Charge (ASAC) reviews determinations of suitability every 180 days. The SAC reviews them annually. In addition, an annual update of records checks outlined in Section 150.3.3.1 will be completed. A record of each suitability determination and updated records checks will be maintained in the CS file outlined in Section 150.3.8. While the CS is active, the control agent will maintain regular contact with the CS to identify any derogatory issues that may affect suitability.

Ensure that copies of all documentation concerning records checks and reviews of suitability determination are forwarded to the NUPM.

Promptly apprise the SAC of any CS information found to be false. If a determination is made not to use a person as a CS, promptly destroy any information collected about the person during the suitability evaluation process.

If OI learns an approved CS is no longer suitable to provide information or operational assistance, promptly terminate the CS relationship. Include a detailed statement of the reasons for such termination in the CS file and provide a copy to the NUPM, which will be forwarded to the appropriate DAIGI/AIGI, if necessary.

150.3.6 Control Agent. The control agent is responsible for the control of the CS. Division management is responsible for ensuring that a control agent introduces alternate control agents to each CS under their control.

150.3.7 Instructions to Confidential Source. Whenever a CS is established, the control agent is required to document that the CS has been advised and understands the extent of his/her activities while assisting OI. The CS will sign TIGTA Form OI 9834, *Instructions to Confidential Source*, to acknowledge his/her agreement to follow and abide by the instructions. The control agent and a witness, usually the alternate control agent will also sign the form. The original form is to be maintained in the CS file and a copy forwarded to the NUPM.

For additional guidance regarding the responsibility of the CS to report payments as income, see Chapter 600, Section 50.

150.3.8 Confidential Source Files. Store the CS documents and photographs in accordance with the provisions of the Department of the Treasury Security Manual, reference Treasury Directive 71-10, in which the information is accessible only to the approving official or authorized alternate. Authorized access can be designated lower, if appropriate.

A copy of the documentation package (*e.g.*, CS Application, Instructions to CS Form, one original set of handwriting exemplars, and one original set of photographs and fingerprints) will be provided to the NUPM by the control agent. All original documentation is maintained by the controlling SAC-/Director. No additional copies will be made or maintained by TIGTA.

150.3.9 Change of Field Division. If a CS moves to a different field division and agrees to continue furnishing information, make arrangements for the receiving field division to establish that individual as a CS.

- Forward the CS file to the receiving SAC-Division.
- The CS will retain the last three digits of the original identifier number since it is not field division specific.

150.3.10 Confidential Source Control Folders. Once a CS designation is approved, the control agent will prepare a CS control folder titled under the CS identifier assigned by the NUPM. Access to the folder is restricted to the control agent, alternate control agent, ASAC, SAC, NUPM, and OI executives. Use a jacket type folder with fasteners on both sides of the interior.

Store CS control folders in accordance with provisions of the Department of the Treasury Security Manual (See Treasury Directive 71-10).

Place the following information on the left side of the folder:

- The report establishing the CS;
- The approval memorandum authorizing the utilization of the CS; and
- Copies of all documents furnished to the investigative Imprest Fund Cashier for payments to or on behalf of the CS, including copies of receipts for payment.

Place on the right side of the folder the following information:

- Reports of all contacts with the CS;
- Record of any information obtained;
- Disposition or uses made of the information;
- Amounts of money paid to or on behalf of the CS, with the date of the Form 1164, *Claim for Reimbursement for Expenditures on Official Business* that were submitted to the Imprest Fund Cashier for reimbursement; and
- In case of negative contacts, an informal memorandum or similar instrument.

Do not place any identifying information other than the assigned number/letter identifier for the CS on documents contained in the control folder.

The Imprest Fund Cashier retains actual receipts (secured in a restricted file) for payment to a CS, with the CS's true name. See Chapter 600, Section 50.

150.3.11 Mailing Procedures for Confidential Source Documents and Information. All CS-related correspondence (*e.g.*, instructions, photographs, fingerprint cards) will be secured within a Restricted File envelope and then shipped via overnight courier service. The shipment must be tracked for receipt and delivery. See Section 190.

150.3.12 Participation in Criminal Activities. Unless approval is obtained as described below, do not authorize a CS to engage in any activity that would constitute a crime under State or Federal law if engaged in by a private person acting without the authorization or approval of an appropriate Government official. For purposes of the following instructions, such activity is referred to as "otherwise criminal" activity.

The approval authority makes the determination that participation by a CS in otherwise criminal activities is justified and only on the basis of his/her written findings that the conduct is necessary to:

- Obtain information or evidence paramount for prosecutorial purposes;
- Establish and maintain credibility or cover with persons associated with criminal activity under investigation; or
- Prevent or avoid the danger of death or serious bodily injury.

This need outweighs the seriousness of the conduct involved. "Extraordinary" and "ordinary" are the two types of otherwise criminal activities for the purposes of these guidelines. The following are the definitions:

- **Extraordinary:** Those involving a significant risk of violence, corrupt actions by high public officials, or severe financial loss to a victim. The appropriate AIGI is the approval authority pertaining to participation in “extraordinary” criminal activity.
- **Ordinary:** The SAC makes a determination that justifies a CS's participation in activities which otherwise would be "ordinary" criminal activities and records it in writing in advance of any such activity. Verbal approval may be given in an emergency situation and confirmed in writing as soon as possible. The NUPM will be immediately apprised when this transpires. The SAC is responsible for reviewing participation in all such criminal activity by a CS.

Note: The authority to approve "otherwise criminal" activity may not be re-delegated.

Determinations authorizing participation in such activities may concern a single instance or a specific group of otherwise criminal activities. Retain the written determinations in both the CS file and the CS control folder.

To the extent practical, ensure that:

- The adverse effect of the activity on innocent individuals is minimized;
- The CS's participation is minimized and is not the primary source of technical expertise or financial support for the activity in which he/she will participate;
- The CS's participation in the activity is closely supervised by OI; and
- The CS does not directly profit from his/her participation in the activity.

150.3.12.1 Consultation with U.S. Attorney Regarding Participation in Criminal Activities. Only the appropriate AIGI can approve participation in activities which are considered to be "extraordinary" criminal activities justified as part of a CS's assignment. The division requesting permission to allow a CS to participate in "extraordinary" criminal activities must consult with and obtain the approval of a U.S. Attorney or an appropriate DOJ official prior to requesting approval from the appropriate AIGI.

The CS's identity is protected during the consultation. Forward the written determination and record of the U.S. Attorney's approval immediately to the appropriate AIGI via the NUPM, in a format suitable to protect the CS's identity.

150.3.12.2 Notification of Unauthorized Criminal Activity. Carefully scrutinize a CS's assignment at all times. If a CS participates in any unauthorized criminal activity, even of a minor nature, promptly apprise the ASAC or SAC, who will brief the NUPM, and the appropriate AIGI.

- The Office of Chief Counsel should be consulted to determine whether notification of State or local authorities is authorized under applicable disclosure laws via the referral procedures in Chapter 700, Section 70;
- The NUPM will annotate the occurrence in the NUPM CS file;
- The appropriate AIGI or DAIGI is apprised of subsequent decisions and developments such as discussions with State or local authorities; and
- Consistent with disclosure guidelines, notify appropriate prosecutors regarding the unauthorized criminal activity.

Do not take any action to conceal a crime by a CS under any circumstances.

150.3.12.3 Acts of Violence. Immediately notify the ASAC or SAC, who will brief the appropriate AIGI or DAIGI and the NUPM whenever a CS participates in a serious act of violence, even when appropriate State or local law enforcement or prosecutorial authorities are aware of the incident.

- Maintain detailed records regarding any instance of CS participation in a serious act of violence; and

- The appropriate AIGI makes the determination to continue use of the CS in consultation with the Assistant Attorney General, Criminal Division, DOJ, as necessary.

150.3.13 Confidential Sources Having Judicially Recognized Privilege of Confidentiality. Do not use a person as a CS if he/she is under the obligation of a legal or generally recognized privilege of confidentiality (*e.g.*, licensed physician, person admitted to practice law, practicing clergy) or is affiliated with the news media, without the written approval of the appropriate AIGI or DAIGI.

The appropriate AIGI or DAIGI promptly gives written notice, or verbal notice confirmed in writing, to the Assistant Attorney General, Criminal Division, DOJ, or his/her designee, of any such OI authorization. The notice includes sufficient information to allow meaningful review, and states the reasons why the individual should be used as a CS.

Advise any such person approved as a CS that, in seeking information from him/her, OI is not requesting and does not advocate breach of any legal obligation of confidentiality.

Prepare a record and keep in the CS file after giving the advisement. Furnish this advisement before accepting information on a continuing basis.

If, despite the advice to the CS that disclosure of privileged information is not requested or advocated, the CS still offers to provide information that is privileged or arguably privileged, do not accept the offer unless the SAC determines that serious consequences would ensue from rejection of the offer (*e.g.*, physical injury to individual or severe property damage). Promptly forward a report concerning such information and the circumstances that warranted its acceptance to the appropriate AIGI or DAIGI.

If the information is spontaneously provided by the CS, without any offer that would alert the SA to the nature of the information, in circumstances that do not meet the standard of serious consequences, record the information to establish that the problem was recognized and that no use was made of the information in the conduct of any investigation.

150.3.14 Confidential Sources Who Are Prisoners. OI investigations may involve the use of prisoners as informants. If using a prisoner as an informant in an investigation, make a request to use the prisoner to the appropriate authority. Prepare the request for signature of the appropriate AIGI. Include the following information:

- Location of the prisoner;
- Identifying data on the prisoner;

- Necessity of utilizing the prisoner in the investigation (provide only that information that is necessary in order to obtain the use of the Federal prisoner);
- Name(s) of the target(s) of the investigation only if it is necessary in order to obtain the use of the Federal prisoner;
- Nature of activity requested;
- Security measures to be taken to ensure the prisoner's safety, if necessary;
- Length of time the prisoner will be needed in the activity;
- Whether the prisoner will be needed as a witness;
- Whether a prisoner re-designation will be necessary upon completion of the activity; and
- Whether the prisoner will remain in the custody of OI or whether he/she will be unguarded except for security purposes.

Address requests for use of Federal prisoners to the attention of the Associate Director, Office of Enforcement Operations, P.O. Box 7600, Ben Franklin Station, Washington, DC, 20044-7600. The Office of Enforcement Operations forwards their recommendation to the Bureau of Prisons (BOP), which advises OI of its decision. Provide a report detailing the results of the activity to the Office of Enforcement Operations within 60 days of its conclusion.

For requests for use of State prisoners, follow the guidelines established by that jurisdiction.

150.3.15 Confidential Sources Who Are Cooperating Defendants. If a CS is developed from a subject who decides to become a “cooperating defendant,” ensure the following:

- Obtain the concurrence of the USAO;
- Comply with all court rulings, if any, regarding the utilization of the CS; and
- If the CS has already been convicted, liaison with the U.S. Probation Officer assigned to the CS to ensure that required monthly reports regarding the activity of the CS are completed.

Provide the U.S. Probation Officer with specific investigative information, such as target names and locations, only if and to the extent that disclosure is authorized by Federal confidentiality laws (*e.g.,* 26 U.S.C. § 6103 and the Privacy Act). See Chapter 700, Section 50.5.2.

150.3.16 Infiltration of Organizations by Confidential Sources. Individual members of legitimate organizations may be independently involved in criminal activities. To ensure that the privacy of constitutionally-protected activities is respected, carefully regulate the

use of a CS who uses affiliation with legitimate organizations to gather information concerning the activities of individual members.

In determining whether the use of such an affiliated person as a CS is viable, the appropriate AIGI or DAIGI, who is the approving official, should consider:

- The likelihood of responsible behavior by the CS during the course of his/her organizational membership.
- The ability of OI to focus the CS's reporting on members of the organization involved in criminal activities and to minimize adverse impact on innocent members of the organization.
- Whether the use of the CS might inhibit free association or expression of ideas by innocent members of the organization in the future, or hinder the ability of the organization to function effectively.

In approving the use of such an affiliated person as a CS, the approving official establishes procedures, recorded in writing, to minimize any acquisition, retention, and dissemination of information that does not relate to the matter under investigation or to any other authorized investigative activity.

150.3.17 Coordination with the U.S. Attorney's Office. Fully disclose to the Federal prosecutor the nature and scope of any CS participation in matters presented to DOJ.

However, if it is necessary to withhold certain information to protect the CS's identity from possible compromise, inform the prosecutor of the general nature of the withheld information. Authority to release the identity of a CS is delegated to the SAC and cannot be re-delegated.

150.3.18 Compensation of Confidential Sources. OI may pay a CS a reasonable amount of money or provide other lawful consideration for:

- Information furnished;
- Services rendered; and
- Expenses incurred in authorized investigative activity.

Do not offer payment of money or other consideration, other than a published reward, that is conditioned on the conviction of any particular individual.

In determining the value of information furnished, consider the following factors:

- Significance of individuals or organizations involved;
- Complexity of investigation in terms of level of penetration and jurisdictions involved;
- Probative value of information;

- Nature or significance of any seizures;
- Investigative time saved through use of informant;
- Time and effort expended by informant;
- Degree of danger involved; and
- Other pertinent factors.

Where practical, state in a compensation agreement with a CS that compensation will depend on compliance with the obligation of confidentiality for investigative information, and that any profits derived from a violation of the obligation shall be forfeited to the U.S.

Payments for services or information to a CS who is an IRS employee are not authorized. However, minimal expenditures, such as for meals or refreshments, are allowed as a liaison expense solely for the purpose of maintaining a relationship between the CS and TIGTA.

Information concerning specific instructions on payments to a CS is contained in Chapter 600, Section 50 of the TIGTA Operations Manual.

150.3.19 Protection of Confidential Sources. Disseminate the identity of a CS and any information that may identify a CS only upon direction of the approving official. In the event that a CS is threatened, OI will assess the threat to determine an appropriate response. If necessary, refer a CS to DOJ for protection and relocation under the Witness Security Program. See Section 230.

150.4 Law Enforcement Databases.
OI uses computerized databases to communicate with other law enforcement agencies and to conduct various criminal history inquiries. This section provides specific information concerning the following databases:

- TECS;
- National Crime Information Center (NCIC);
- National Law Enforcement Telecommunications System (NLETS); and
- El Paso Intelligence Center (EPIC).

150.4.1 TECS. TECS is a computerized data processing system designed to identify individuals involved or suspected of involvement in violation of U.S. laws. TECS is maintained by the Department of Homeland Security, U.S. Customs & Border Protection (CBP), Office of Information Technology.

TECS comprises several databases containing law enforcement-related information.

TECS provides direct access to the NCIC and NLETS. Specific information concerning TECS and directions for TECS use are for "Official Use Only." This information is provided on TECS system and is available only to authorized users.

NCIC and NLETS entries and queries shall only be made through TECS.

150.4.2 National Crime Information Center. NCIC is an electronic clearinghouse for crime data available to all local, State and Federal criminal justice agencies nationwide.

NCIC regulations require that the agency having primary jurisdiction over the offense make all necessary entries into NCIC. The agency must have written documentation, such as a report, to make an entry.

Temporary felony want records allow persons, in exigent circumstances, to be entered for 48 hours without a warrant.

The system also contains images that can be associated with NCIC records to help agencies identify people and property items.

150.4.3 Sensitivity of TECS and NCIC Data. All TECS and NCIC data, excluding TECS Interstate Identification Index (III), is designated as "Law Enforcement Sensitive For Official Use Only." Information from the TECS III files is "Limited Official Use Only." Mark all printouts with the appropriate classification. Shred or burn them when no longer needed.

The TECS and NCIC information is owned by the originating agency. This information must be verified by the originating agency and cannot be used in ROIs or disseminated outside of OI law enforcement without the originating agency's approval.

Do not attach TECS or NCIC printouts to ROIs or other types of correspondence disseminated outside of OI. Use the TECS and NCIC information only as lead information. Agents must verify the information by obtaining the source document(s) from the law enforcement agency or court before including it in the ROI or other correspondence. See Section 250.

For Potentially Dangerous Taxpayer (PDT) determinations do not provide the IRS-Office of Employee Protection with information obtained only from TECS or NCIC. Such information may not be provided outside of OI without verification by the originating agency prior to such a disclosure.

Indirect dissemination of information contained in NCIC files, other than from TECS III, is not prohibited, but must be approved by the Criminal Justice Information Services (CJIS) program manager who also serves as TIGTA's Terminal Agency Coordinator (TAC) and National Systems Control Officer (NSCO).

TECS III information may not be disseminated except for criminal justice purposes, and may not be disseminated outside of TIGTA.

150.4.4 NCIC Messages. The six types of messages pertaining to NCIC records are:

- Entry: enters a new record into NCIC or provides supplemental information to an existing record;
- Modification: adds, deletes or changes data in an existing record;
- Locate: notification that an agency has recovered a stolen item or apprehended a fugitive;
- Cancellation: removes an invalid record, restricted to the originating office;
- Clear: notification that an item or individual may be removed from the system because enforcement action has been taken; and
- Inquiry: requests the system to check one or more databases for the existence of active records.

150.4.5 Control Terminal Agency. A Control Terminal Agency is a Federal, State or territorial criminal law enforcement agency on the NCIC system providing Statewide or equivalent service to its NCIC users. TIGTA's Control Terminal Agency is the CBP.

150.4.6 NCIC Hit. An NCIC "hit" is a positive response to an inquiry. Immediately confirm with the originating agency all NCIC queries that result in a hit by entering an administrative message into NLETS or by a telephone call. Enter all confirmed hits into NCIC as a Locate message. The person initiating the query must ensure the Locate message is entered. NCIC regulations require TIGTA to ensure someone is available 24 hours a day, seven days a week to confirm a "hit" on all records, except TECS III records.

150.4.7 Arrest Based on NCIC Hit. An NCIC hit is not probable cause to make an arrest. Contact the originating agency to verify the record.

150.4.8 Ten Minute Hit Confirmation Policy. OI requires a 10-minute response time for its records. "Confirming a hit" means contacting the agency that entered the record to:

- Ensure that the person or property inquired about is identical to that identified by the record;
- Ensure that the warrant, missing person report or lost or stolen property report is still outstanding; and
- Obtain a decision regarding the extradition of a wanted person, information regarding the return of the missing person to the appropriate authorities, or information regarding the return of stolen property to its rightful owner.

Upon receipt of a hit confirmation request, an originating agency must furnish the requesting agency one of the following within 10 minutes:

- A positive confirmation;
- A negative confirmation, reject; and
- Notice of the specific amount of time necessary to confirm or reject.

********** provides "hit" confirmation for TIGTA arrest warrants. If the TECS user receives such a notice, ********** to obtain the name of the responsible TIGTA case agent. For all other "hit" confirmations, the primary point of contact identified on the *TIGTA Lost/Stolen Article Form* will be contacted.

150.4.9 NCIC Off-line Searches. An NCIC offline search inquiry is a special query of NCIC for information, which cannot be obtained through the use of online inquiries. The offline search is made against two sources of NCIC information: online files and historical data such as records that have been removed from NCIC transaction logs. Only FBI NCIC officials may conduct offline searches.

150.4.10 National Law Enforcement Telecommunications System. NLETS' purpose is to provide an improved interstate law enforcement and criminal justice communications system. NLETS provides a message service and supports inquiry by users into State records such as motor vehicle, driver's license, criminal history, and other State databases. NLETS consists of representatives of law enforcement agencies from each of the 50 States, the District of Columbia, Puerto Rico and several Federal law enforcement agencies.

NLETS is a computerized, high-speed message switching system created for and dedicated for use by the criminal law enforcement community. NLETS provides for interstate or interagency exchange of criminal justice or related information and messages.

150.4.11 National Law Enforcement Telecommunication System Query Files. NLETS can be queried for out-of-State information using the following files:

- Driver's License;
- Driver History;
- Vehicle Registration;
- Criminal History;
- Road/Weather Conditions;
- Administrative Messages;
- Boat Registration;
- Snowmobile Registration;
- Hazardous Material;

- Federal Aviation Administration (FAA)/TECS Aircraft Tracking System; and
- FAA/TECS Aircraft Registration System.

150.4.12 CJIS Program Manager. The CJIS program manager:

- Serves as TIGTA's point-of-contact for all matters relating to CJIS access;
- Serves as the OI point-of-contact for all CJIS-related matters and provides technical and policy guidance on the security and use of CJIS and data;
- Administers CJIS programs within TIGTA and oversees the agency's compliance with CJIS policies;
- Monitors CJIS use, enforces CJIS discipline, and assures proper procedures are followed;
- Ensures compliance with national, State, and local NCIC policies, rules, and regulations through routine review and analysis of CJIS use;
- Maintains liaison with State and Federal CJIS Systems Officers and other local TACs;
- Provides input into State and Federal networks and the national NCIC system;
- Trains and certifies operations, maintains system records, validates records, performs quality control reviews, enters/modifies/clears/cancels records, and provides technical and operational assistance;
- Provides oversight of and support to TIGTA's Systems Control Officers;
- Establishes policies and guidelines for user profile records and permission levels;
- Ensures monthly NCIC data validations are completed and returned to NCIC timely;
- Reports all significant administrative and program weaknesses discovered during audits, validations, or quality control reviews; and identifies appropriate corrective actions; and
- Formulates, modifies, and recommends policies, procedures, systems, and methods for the effective management of CJIS.

150.4.13 Systems Control Officer. Each field division has one or more SCOs. SCOs provide support to the CJIS program manager in maintaining compliance with TECS/NCIC rules and regulations. SCOs:

- Provide support to the CJIS program manager to ensure field compliance; and
- Provides support to the TECS users such as unlocking profiles, extending training certification dates, resetting passwords, assisting with queries, assisting with inputting and/or modifying records, and contacting BCP to make profile adjustments.

150.4.14 Oversight. The CJIS program manager reviews the operations of SCOs and is responsible for correcting all instances of noncompliance by SCOs and users.

150.4.15 User Profile Records. The User Profile Record (UPR) creates the account and consists of identifying information and documentation of training required for TECS use. The CJIS program manager must prepare a UPR to create the account to access TECS.

All SAs with UPRs have access to complete "Inquiry," "Locate," and "Entry" messages.

150.4.16 TECS User Criteria. Each TECS user must have a UPR and an account to use TECS. The user must then pass TECS online computer generated training courses.

The CJIS program manager may provide the UPR and account to an SA or other TIGTA-OI employee determined to have a business need to access the system.

Cooperative student employees, interns, seasonal and temporary employees may not be granted access to TECS.

To request a UPR account, the employee must complete TIGTA Form 5081, *TIGTA Information Systems User Registration/Change Request*, and the employee's manager must submit the form to the CJIS program manager.

Before access will be granted, the employee must have:

- A background investigation completed within the preceding five years;
- Complete all required TECS training courses; and
- Legitimate need for access to TECS.

150.4.16.1 Removing a TECS User. When an employee no longer needs access to TECS, separates from TIGTA, or is under investigation, the employee's manager will complete TIGTA Form 5081 requesting to suspend and/or remove the TECS user's access. Send TIGTA Form 5081 to the CJIS program manager for processing.

150.4.17 TECS Liability. The person who enters data, or requests that information be input to TECS, is responsible for the accuracy and completeness of the record. The requester or user who input the record is responsible for removing a record from TECS once it is no longer valid.

The requester or TECS user may be held civilly liable for failure to remove invalid records. For example, if a wanted person is arrested a second time because the original record was not removed after the first arrest, the SA who made or requested the TECS entry may be held responsible.

150.4.18 Audit Trails. TECS generates audit trails on each user from log-on to log-off. Each screen seen by the user and all information typed on the screen are maintained online. The CJIS program manager requests all audit trails through CBP, Office of Internal Affairs.

150.4.19 Query Logs. NCIC requires each agency to maintain a manual or automated log of all queries for a minimum of one year. The automated audit trails maintained by TECS meet this requirement.

A log to document secondary disclosure of criminal history record information must also be maintained. All criminal history record inquiry requests must show to whom the information is to be delivered. This information can be maintained in the TIGTA Form OI 6501, *Chronological Case Worksheet*.

150.4.20 Security. A shredder or Agency-provided "shred bin" must be available to destroy unwanted printouts. Use a safe or locking cabinet to store all printouts containing criminal history data.

150.4.21 OI Entry Procedures. All TECS and NCIC entries, except arrest warrants, are completed by the case agent.
**********.

The case agent will send a completed Article Form and the NCIC entry record to the CJIS program manager. Include the intake or investigation number in the subject line of **********.

The TECS user will insert the case agent's last name and cell phone number when inputting any articles into NCIC. The TECS user must insert the disclaimer to contact the ********** to obtain the name of the responsible TIGTA case agent. If another law enforcement agency is the lead, that agency will input items.

150.4.21.1 Arrest Warrants. TECS/NCIC policy requires that all arrest warrants be input immediately into the system. This requirement is to ensure the safety of other law enforcement officers who may be in contact with the subject.

****** will enter arrest warrants for TIGTA upon receipt of a valid request and supporting documentation. The case agent will send a completed **********, a valid arrest warrant that is signed by the Judge, the **********, and a photo of the subject to the appropriate National Law Enforcement Communications Center at CBP. Addresses can be found on the Technical and Firearms Support Division's (TFSD) intranet page.

150.4.21.2 Lost Credentials. Do not input lost or stolen IRS credentials (*e.g.,* proximity badges, SmartID badges, IRS pocket commissions).

150.4.21.3 OI Arrest Warrant Removal Procedures. TECS/NCIC requires that all executed arrest warrants be removed immediately from the system to prevent other law enforcement entities from mistakenly arresting the subject under the belief that the warrant is still active. TIGTA defines immediate removal as requiring the SA executing the arrest warrant or another designated agent to contact ********** and request that the warrant be removed.

150.4.21.4 Validations. OI is responsible for ensuring the accuracy, timeliness and completeness of all records it enters into TECS and NCIC.

All items entered into NCIC are subject to a monthly validation of records procedure. NCIC officials periodically prepare a listing from the database and forward the data to the entry agency for verification. To validate these items, an agency must ensure that each of the following is verified:

- Supporting documentation is present;
- All fields are completed;
- All information is correct;
- Case is still pending; and
- Wanted persons/fugitives are still at large, verified by completing a court house check to ascertain that the warrant still exists.

The SCO advises the CJIS program manager, who is responsible for providing NCIC a signed statement that the sample data was validated and correct. Failure to comply will cause the entry to be deleted.

150.4.21.5 El Paso Intelligence Center. The EPIC is a multi-agency operation that collects, processes and disseminates information in support of ongoing field investigations. EPIC's primary mission is to provide an accurate intelligence picture of drug movement by land, sea and air throughout the world.

150.4.21.6 EPIC Requests. All EPIC requests are made through TECS access. The request must be in connection with an investigation which involves narcotics, drug related money laundering, illegal alien or weapons smuggling activities.

If available, include the following identifying information:

- Suspect's aliases;
- Suspect's Place of Birth;
- Suspect's parents' names;

- SSNs;
- Driver's license information;
- Passport information;
- Suspect's street address and telephone numbers;
- Company name, address, and telephone numbers;
- Alien registration number;
- FBI number; and
- Race, sex, height, weight, color of hair and eyes.

Agency requests to EPIC are recorded in EPIC's database. A permanent entry, which reflects the particulars of the inquiry, is maintained in the subject's record.

150.5 Mail Covers.
A mail cover is the process by which a nonconsensual record is made of any data appearing on the outside cover of sealed or unsealed class of mail matter, or by which a record is made of the contents of any unsealed class of mail matter as allowed by law.
****
**********.

150.5.1 Requests for Mail Covers. **********
****
****
****
****
********.

****
****
**********.

150.5.2 Return of Mail Cover Information. **********
****
****
****
****
********.
150.5.3 Cancellation of Mail Covers. Cancel a mail cover when the information sought is obtained.

150.5.4 Documentation of Mail Covers.
****
****
****
********.

150.6 Taxpayer Data.
SAs may need to obtain original tax returns, return information, audit reports, and IRS Criminal Investigation (CI) reports from the IRS if investigating a violation of Title 26 or a related statute. This information may only be obtained if the SA is performing a tax administration investigation. See Chapter 700 for a discussion of the authority to access tax returns and return information.

150.6.1 Tax Returns and Return Information. Use the Integrated Data Retrieval System (IDRS) to order and control tax returns and return information required during a tax administration investigation. SACs are responsible for ensuring there are adequate controls over the approval of requests for returns and return information and that returns and return information are promptly returned to files when they have served their purpose. Requests for all other tax records, or those that cannot be generated through IDRS, may be requested using IRS Form 2275, *Records Request, Charge and Recharge*.

150.6.1.1 Control Procedures. OI will follow all procedures that the IRS requires when they request tax returns and/or return information.

When tax returns or return information are requested, it is the responsibility of the SAC-Field Division to ensure that:

- There are adequate controls for approving SA requests for returns and/or return information; and
- SAs promptly return to the IRS original tax returns and/or return information when they are no longer needed.

Whenever possible, SAs should promptly make working copies of original tax returns and/or return information obtained from the IRS, and return the originals to the IRS for storage and safekeeping. Original tax returns maintained by TIGTA as evidence will be processed in accordance with Section 190.

150.6.1.2 Use of Third Party Returns or Return Information. It is sometimes necessary to disclose authentic third party tax returns or return information to non-IRS employees, especially during undercover operations. The returns or return information may be disclosed only after:

- Securing the third party's consent. See TIGTA Form OI 1933, *Consent for Release of Tax Return and/or Return Information by the Treasury Inspector General for Tax Administration*; and
- Discussion with TIGTA Counsel if unable to secure the third party's consent to determine if 26 U.S.C. § 6103 would authorize the disclosure under the circumstances at issue.

150.6.2 IRS Tax Audits or Criminal Investigation Reports. To review a tax audit report or an investigative report by IRS CI, contact the IRS management official overseeing the function. Include a copy of portions of the tax audit or investigative report in the TIGTA report only if pertinent to the case.

150.7 Centralized Authorization File.
The Centralized Authorization File (CAF) is an automated file available on IDRS of taxpayers that have executed powers of attorney and contains the names of taxpayers' representatives. Use CAF information only for OI investigative purposes. To receive a CAF, submit a Request Assistance Form (RAF) in CRIMES.

150.7.1 Accessing the Centralized Authorization File. SAs who are authorized to use IDRS are also authorized to make ordinary IDRS inquiries of the CAF in connection with their official duties. SAs must comply with the provisions of 26 U.S.C. § 6103 when accessing tax returns and return information, including information in the CAF concerning taxpayer representatives received by the IRS on filed tax returns.

150.7.2 CAF Analysis and Utilization. CAF data may be used:

- As an investigative tool to identify former and current clients of representatives;
- To provide for the security of IRS employees after a representative is designated as a PDT and additional contacts with the representative are anticipated;
- To identify clients of a representative after the representative has made a bribe overture in order to identify other potential bribe overtures; or
- For further analysis with other IDRS information to identify IRS employees who were assigned cases in the names of clients whose representative made a bribe overture.

Do not use CAF data to initiate audits if the information is available through another source, such as the Preparer Inventory File, or the Automated Information Management System historical files.

150.8 Information from State or U.S. Territorial Taxing Authorities.
SAs may need copies or originals of tax returns or return information filed with State or U.S. territorial (*e.g.*, Puerto Rico) taxing authorities during the course of their investigations.

150.8.1 Request Procedures. To obtain copies or originals of tax returns or return information filed with State or U.S. territorial taxing authorities, OI will take the necessary steps to acquire the information in the order listed below:

- Direct request to taxing authority;
- Request for assistance from IRS Disclosure Office; and
- Subpoena request.

150.8.1.1 Direct Request to Taxing Authority. SAs will make a request to the State/territorial taxing authority, in writing if necessary, that the identified tax return or return information is necessary for the investigation of a Federal matter under the authority of TIGTA.

150.8.1.2 Request for Assistance from IRS Disclosure Office. The IRS has memoranda of agreement with all State and territorial taxing authorities authorizing it to receive tax returns or return information filed with the State/territorial taxing authority, provided such information is required for the purpose of tax administration. IRS will assist TIGTA in obtaining tax returns or return information filed with State and territorial taxing authorities provided that the SA is performing a tax administration investigation pursuant to Title 26 or related statutes, and that tax returns or return information provided is protected by the confidentiality provisions of 26 U.S.C. § 6103. Consult TIGTA Counsel and/or see Chapter 700 for a complete discussion of 26 U.S.C. § 6103.

In the event the State or territorial taxing authority refuses TIGTA's request for tax return or return information, SAs will direct their request to the appropriate IRS Disclosure Office, provided that the records sought are necessary for an official investigation related to Federal tax administration. SAs will take the following action:

- Complete IRS Form 8796, *Request for Return/Information*, Sections A and B. Regarding Section C, complete Block #1 (requesting SA), Block #2 (SAC), and Block $4 (address). DO NOT complete Block #3, as it will be completed by the authorizing IRS Disclosure Officer.
- Complete a very brief memorandum addressed to the IRS Disclosure Office stating that TIGTA is conducting an official investigation related to Federal tax administration and that requested material will be protected according to the provisions of 26 U.S.C. § 6103. Provide only enough information so that the addressee knows what records are needed for the investigation. The memorandum should not provide details related to the nature of the investigation, as the memorandum will be provided to IRS and the State/territorial taxing authority.
- Submit both the IRS Form 8796 and memorandum to the appropriate IRS Disclosure Office via facsimile.

State/territorial taxing authorities typically will respond within four to six weeks.

150.8.1.3 Subpoena Request. In the event TIGTA is unable to obtain the necessary records through the State/territorial taxing authority or IRS, the SA requiring such

records should contact the Operations Division to discuss the use of an administrative subpoena. See Section 220.

150.8.2 Control Procedures. When tax returns or return information are requested, it is the responsibility of the SAC to ensure that:

- There are adequate controls for approving SA requests for State/territorial tax returns and/or return information.
- SAs promptly return to State/territorial taxing authorities all original documents when no longer needed.

150.9 Social Security Administration Account Information.
The Social Security Act authorizes the Social Security Administration (SSA) to disclose information to any officer or employee of the Department of the Treasury lawfully charged with administering the following laws or regulations:

- Social Security Act, Titles II, VIII, IX;
- Self-Employment Contributions Act;
- Federal Unemployment Tax Act; and,
- Any Federal income tax law.

The regulations forbid further disclosure of information or its use for purposes other than the administration of the above-cited laws. To obtain SSA account information contact the local SSA office or the SSA Office of the Inspector General.

150.10 Obtaining Wage or Other Income Statements.
Request wage and other income statements through the IRS Information Returns Processing (IRP) System. IRP information is available beginning with calendar year 1977 and retrievable only by SSN. It is important to note, however, that this information may only be obtained from the IRS if the SA is performing a tax administration investigation, pursuant to Title 26 or related statute. This information may be obtained by submitting a RAF in CRIMES or using command code “IRPTR” in IDRS.

See Chapter 700, Section 120 for a discussion of the authority to access tax returns and return information.

150.11 Information Available Under the Bank Secrecy Act.
The Bank Secrecy Act (BSA), originally the Currency and Foreign Transactions Reporting Act of 1970, requires financial institutions to keep a number of different types of records (including records of cash purchases of negotiable instruments), file a number of different types of reports (including of cash transactions exceeding a daily aggregate amount of $10,000, and of suspicious activity that might signify money laundering, tax evasion, or other criminal behavior), and to maintain anti-money laundering programs.

150.11.1
****
****
****
****
**********.

****
**********:

Report	Requirements
**********	Filed by financial institutions that engage in a currency transaction in excess of *******.
**********	Filed by a casino to report currency transactions in excess of *******.
**********	Filed by individuals to report a financial interest in or signatory authority over one or more accounts in foreign countries, if the aggregate value of these accounts exceeds ********* at any time during the calendar year.
**********	Filed by persons engaged in a trade or business who, in the course of that trade or business, receives more than ******** in cash in one transaction or two or more related transactions within a twelve-month period.
**********	Filed on transactions or attempted transactions involving at least ****** that the financial institution knows, suspects, or has reason to suspect that: the money was derived from illegal activities; the transaction was part of a plan to violate Federal laws and financial reporting requirements (structuring); or the transaction has no business or apparent lawful purpose or not typical for the customer and the financial institution doesn't know of a reasonable explanation for it.

**********	Filed on transactions or attempted transactions if it is conducted or attempted by, at, or through a casino, and involves or aggregates at least ****** in funds or other assets, and the casino/card club knows, suspects, or has reason to suspect that the transactions or pattern of transactions involves funds derived from illegal activities. Also filed when transactions are part of a plan to violate Federal laws and transaction reporting requirements (structuring).

150.11.2 Disclosure of ********** and Underlying **********.
The disclosure rules for information gathered during the course of a ********** compliance activity are different from information prepared or received pursuant to Title 26. Title 26, U.S.C. § 6103 prohibits the sharing or disclosure of tax returns and return information prepared or received pursuant to Title 26 unless a specific exception applies under § 6103.

The unauthorized disclosure of a *** is not only a violation of Federal criminal law, but it undermines the very purpose for which the suspicious activity reporting system was created – the protection of our financial system through the prevention, detection, and prosecution of financial crimes and terrorist financing.

Federal law (31 U.S.C. § 5318(g)(2)) prohibits the notification of any person that is involved in the activity being reported on a *** that the activity has been reported. This prohibition effectively precludes the disclosure of a *** or the fact that a *** has been filed. However, this prohibition does not preclude, under Federal law, a disclosure in an appropriate manner of the facts that are the basis of the ***, so long as the disclosure is not made in a way that indicates or implies that a *** has been filed or that the information is included on a filed ***.

There is a narrow exception that allows a Special Agent (SA) to disclose the existence of a *** in fulfilling his official duties, but FinCEN has interpreted this exception to apply only when it is *required* that the *** be disclosed, for instance, in the course of a criminal trial in order to comply with constitutional due process requirements.

****
****
****
****
****
**********.

150.11.3 Financial Institution Disclosure of *** Documentation.
****
****
****
****
****
****
**********.

150.12 National Instant Criminal Background Check System.
The National Instant Criminal Background Check System (NICS), a system owned by the FBI, was implemented in 1998 for the purpose of enhancing national security and public safety by providing the timely and accurate determination of a person's eligibility to possess firearms and/or explosives in accordance with Federal law. The NICS Improvement Amendments Act (NIAA) of 2007 and the Fix NICS Act of 2017 have further defined agencies' reporting responsibilities. Federal agencies are required to make all applicable records electronically available to NICS on a regular basis, and to submit semiannual certifications to the Attorney General.

150.12.1 Persons Prohibited from Possessing or Receiving a Firearm. The implementation of NICS has been instrumental in denying the transfer of firearms to criminals and other persons for whom possession is against the law. However, the ability of the NICS personnel to make a quick and effective determination as to whether an individual is prohibited from possessing a firearm depends on the completeness and accuracy of information made available by Federal, State, and tribal authorities. There are 10 categories of persons who are prohibited from possessing or receiving a firearm by Federal law:

- Felons;
- Fugitives from justice;
- Persons unlawfully using or addicted to any controlled substance;
- Persons adjudicated "mentally defective" or committed to a mental institution;
- Illegal/unlawful aliens, and aliens admitted on a non-immigrant visa;
- Persons dishonorably discharged from the military;
- Citizen renunciates;
- Persons subject to a domestic violence restraining order;
- Persons convicted of a misdemeanor crime of domestic violence; and/or
- Persons under indictment/information (for a crime punishable by imprisonment for a term exceeding one year).

150.12.2 Databases Available to NICS Personnel. **
***:

- **;
- **; ***
- **.

150.12.3 Responsibilities. OI's TFSD administers OI's compliance with NICS. In order to accomplish OI's compliance, TFSD works with OI Divisions to ensure timely and accurate reporting.

150.12.4 Field Division Personnel Responsibilities. Upon arrest, surrender, or booking of a subject, the case SA must ensure the correct Originating Agency Identifier (ORI) is entered in the U.S. Marshals Service's Joint Automated Booking System (JABS). See Section 140.5.10, *Fingerprinting, Booking, and DNA Sampling,* provides instructions on TIGTA's unique ORI and how to locate it in JABS.

SAs must also ensure fact sheets for any legal actions are submitted without delay, in accordance with Section 30.7, *Reporting Significant Cases.* The fact sheet shall contain all available information, such as literal charges by statute and supporting court documents, whenever possible. If documents are under seal or otherwise protected, such information must be clearly stated in the fact sheet. *********************************
***************************.

SAs are responsible for entering all relevant legal actions into CRIMES in an accurate, complete and timely manner. See Section 80.

It is the responsibility of the reviewing ASACs and SACs to ensure the accuracy and timeliness of CRIMES data and fact sheet content and submissions.

150.12.5 Technical and Firearms Support Division Personnel Responsibilities. TFSD serves as the NICS program manager and is responsible for monitoring internal compliance and ensuring the accuracy of arrest records relative to TIGTA investigations *** and/or State and local law enforcement agencies, as well as the transmission of disposition information and updates via FBI Forms R-84, *Disposition Reports,* to CJIS as required. Records that cannot be entered into ******************, but have relevance for prohibiting factors, will be entered into the NICS Indices database ***, or otherwise provided to NICS personnel. The NICS program manager will also be responsible for correcting any deficiencies identified in coordination with CJIS.

The NICS program manager will verify all new arrest records and identify final disposition information no less than quarterly and submit records to the FBI/CJIS within 15 days after the end of each quarter, whenever possible. Additionally, the NICS program manager will monitor internal compliance through the continuous, but no less than quarterly, reviews of legal actions.

To avoid duplicative efforts and to ensure dispositions are appropriately reported, the NICS program manager is the only authorized component within OI to submit Forms R-84 to the FBI.

The NICS program manager will additionally maintain coordination with divisions to ensue Form R-84 submission data is provided for the NICS biannual certifications. The NICS program manager will also coordinate with FBI, if requests are made regarding outstanding disposition records. In addition, the program manager will maintain coordination with the TFSD NICS program manager to collect the necessary information to prepare the NICS biannual certifications for the Attorney General. The first certification is due no later than January 31 of each calendar year and covers the period July 1 through December 31, of the prior calendar year. The second certification of each year is due no later than July 31, and covers the period January 1 through June 30.

DATE: July 1, 2020

CHAPTER 400- INVESTIGATIONS

(400)-160 Technical Investigative Support

160.1 Overview.
The Technical and Firearms Support Division (TFSD) provides technical investigative support for investigative and enforcement operations. TFSD consists of two groups, Enforcement and Technical Operations and Investigative Support. Requests for technical investigative support are initiated by submitting a Request Assistance Form (RAF) in the Criminal Results Management System.

This Section includes the following information:

160.1.1 Acronyms Table.

160.2 Authority for Use.
Title 18 U.S.C. §§ 2510 – 2522 provides the authority for the use of technical investigative equipment to monitor communications during investigative and enforcement operations. Permission to use electronic monitoring equipment is limited to investigations involving alleged violations within Treasury Inspector General for Tax Administration's (TIGTA) jurisdiction.

There are two types of monitored communications, consensual and non-consensual. Consensual monitoring is the interception by an electronic device of any wire, oral, or electronic communication for which one of the parties to the communication has given prior consent to the monitoring or recording. A warrant is not required to conduct consensual monitoring and the party providing consent may be a Government agent. Non-consensual monitoring requires a court order pursuant to Title I of the Electronic Communications Privacy Act of 1986. See Section 170 for additional information related to non-consensual monitoring.

The U.S Department of Justice *Attorney General Guidelines for Offices of Inspectors General with Statutory Law Enforcement Authority, dated December 8, 2003*, establishes procedures for intercepting, overhearing, transmitting, and/or recording non-telephone conversations, with the consent of at least one of the parties.

160.3 Types of Equipment and Services.
The following are types of technical investigative equipment available from TFSD:

- Global Positioning System (GPS) trackers;
- Body worn cameras;
- Audio/video recorders;
- Cameras; and
- Surveillance platforms.

TFSD has the ability to perform cellphone mapping and analysis using information from cell towers, pen registers, link analysis using cellphone and social media data, and recording consensually monitored telephone calls using existing cellphones. TFSD can turn any cellphone into an audio transmitter or "body bug" for consensual monitored meetings. The cellphone will record the conversation as evidence and as many as 12 special agents (SA) can listen to the conversation simultaneously. TFSD also uses software that can quickly search large volumes of video surveillance footage based on specific parameters provided by the case SA.

160.4 Divisional Technical Agents.
Divisional Technical Agents (DTAs) are assigned to TFSD and report to the Assistant Special Agent in Charge (ASAC)-Enforcement and Technical Operations. DTAs are located in field offices nationwide to facilitate the timely delivery of technical support to field operations. DTAs are Certified Technical Investigators and are certified to work around high-voltage distribution systems.

160.4.1 Divisional Technical Agent Duties. DTAs serve as advisers to the Special Agent in Charge (SAC)/Directors of their assigned division(s) on policies, procedures and legal standards governing the use of technical equipment, and provide technical planning and equipment support to undercover operations, monitored meets, consensual monitoring, enforcement operations and investigations. DTAs may perform complex or covert installations of surveillance systems and devices (See Exhibit (400)-160.1) and are responsible for maintaining the inventory of technical investigative equipment assigned to TFSD.

160.4.2 Technical Services Officer. Technical Services Officers (TSOs) are selected by the SAC/Director of their Division. TSOs assist DTAs in providing technical support for investigative activities and may perform installations of covert surveillance equipment. TSOs process and ensure proper control of evidence obtained through the

use of this equipment. Only a designated TSO may operate sensitive technical equipment. TSO's are required to attend TFSD-mandated training as appropriate.

160.4.2.1 Technical Services Officer Qualifications. The SA selected as the TSO must successfully complete TIGTA's Office of Investigation (OI) Basic Investigative Equipment Training. Completion of TIGTA's Advanced Technical Training Course is recommended. TSOs may receive on-the-job training from the DTA and/or senior TSOs. Refresher training is offered by TFSD as new equipment and technologies are adopted.

Training is required to develop and maintain the TSOs expertise and proficiency. TSOs with limited operational opportunities require training to obtain exposure to proven and updated methods as well as new technologies.

160.5 Electronic Tracking Devices.
Use of electronic tracking device requires appropriate legal approvals, administrative authorization and assistance from TFSD.

TIGTA utilizes two types of electronic tracking devices in support of investigations:

- Radio Frequency devices that employ a series of tones and pulses useful for directional real-time tracking of packages or vehicles; and
- GPS devices that employ satellite telemetry and mapping software to locate the precise longitude and latitude of packages or vehicles in both historical and real-time perspectives.

160.5.1 Electronic Tracking Device Authorizations. In most instances, when TIGTA does not have the consent of the person who is the owner of the property or vehicle, a search warrant authorizing installation and use of a tracking device is required. SAs must discuss the specific legal requirements of the proposed installation with a local Assistant United States Attorney (AUSA) prior to utilizing this technique. The installation and use of tracking devices is covered under Rule 41 of the Federal Rules of Criminal Procedure and specifically pursuant to 18 U.S.C. § 3117, *Mobile Tracking Devices*.

Note: Certain GPS tracking devices are capable of audio and video recording and may require a Title I court order. SAs must discuss the use of this technique with a local AUSA and document the discussion and decision in the case file. See Section 170 for additional information related to Title I intercepts.

The use of electronic tracking devices must be approved by the division SAC/Director. This approval will be documented via TIGTA Form OI 7503, *Operational Plan for Search Warrant*. Absent a search warrant, the SA will prepare a memorandum to the SAC/Director outlining the proposed use of an electronic tracking device and other

resources required to track the target package or vehicle. The memorandum must include the following information:

- Case name and number;
- Complete description of target package or vehicle;
- Proposed duration of tracking;
- Results of initial conference with AUSA;
- Justification for use of electronic tracking device; and
- Proposed surveillance plan.

The SA will retain the original request in the case file and forward copies to the ASAC-Enforcement and Technical Operations and the assisting DTA.

In urgent cases, approval to use an electronic tracking device may be made by telephone. This must be followed as soon as possible by written documentation as previously described.

SAs should begin the process for requesting use of an electronic tracking device by consulting with the DTA assigned to their division. The DTA will assist the SA in gathering certain technical information, planning the installation of equipment, projecting costs and formulating a proposed surveillance plan.

160.5.2 Court Approval of Electronic Tracking Device Procedures. In most cases, a search warrant is required to utilize an electronic tracking device. The SA must contact a local AUSA to obtain advice concerning the legal authorization required to utilize this technique. If a search warrant is required, the SA must prepare an affidavit in support of the search warrant containing the following three critical elements:

- A recitation of the probable cause leading the affiant to believe the property or vehicle will be used in furtherance of a crime in violation of Federal laws investigated by TIGTA;
- An explanation of how the success of the surveillance depends upon the tracking device; and
- Authorization to access the property or vehicle to install and remove the tracking device.

The duration of a search warrant authorizing installation of a tracking device is 45 days and requests for extension may be made. It is recommended that such court orders be “sealed,” when possible, to preserve the integrity of the investigation.

160.5.3 Electronic Tracking Device Installation and Operation. Upon notification that a search warrant has been obtained and a tracking request has been approved by the SAC, the assigned DTA will:

- Determine the method of installation;
- Coordinate the cover team during installation of equipment on vehicles;
- Operate and maintain the monitoring location and equipment; and
- Provide technical advice to the case agent, management, and AUSA.

The SA requesting use of a GPS tracking device:

- Preserves all evidence produced by the GPS mapping software;
- Maintains surveillance logs; and
- Coordinates surveillance teams when required.

160.5.4 Consensual Use of Electronic Tracking Devices. When the owner of the property has given permission for the installation of an electronic tracking device, follow all requirements for requesting approval, with the exception of obtaining a search warrant. Document the owner's consent in writing and ensure that the consenting party is lawfully authorized to give consent.

Note: Tracking of a government-owned vehicle may involve issues related to "reasonable expectation of privacy." SAs must consult with a local AUSA prior to such installation.

For the safety and protection of undercover agents, use of tracking devices on undercover vehicles is an option that should be discussed in all undercover pre-operational meetings. This is considered a consensual use of an electronic tracking device and requires no search warrant.

160.6 Video Monitoring.
Video monitoring and recording is an effective tool in gathering evidence of criminal activity and administrative misconduct. The use of closed circuit television and/or video equipment for monitoring and recording activities may raise legal issues regarding a subject's reasonable expectation of privacy and is governed by the Fourth Amendment. When a reasonable expectation of privacy exists, a search warrant should be sought pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure, and the All Writs Act (28 U.S.C. § 1651). SAs should be guided by the opinion of a local AUSA or appropriate Department of Justice (DOJ) attorney concerning the use of such video monitoring. See Section 140.12 for additional information related to conducting physical surveillance.

160.6.1 Video Surveillance of Public View Areas. Use of a video camera to observe activity that is viewable by the public (either because members of the public can lawfully access the area where this activity occurs or can see the activity from a lawful vantage point) does not generally constitute an intrusion into a constitutionally protected private interest. A warrant is generally not required to visually record activities that occur in

publicly accessible areas such as public parks, sidewalks, streets, open fields, and other areas outside the curtilage of a house that is commonly accessible to the public.

SAs may, without a search warrant, use video surveillance to assist them in observing certain areas even when the areas are within the curtilage of a house if others can observe these same areas from a place they are lawfully entitled to be, such as from the street, sidewalk, or an open field. This would include unobstructed video surveillance of driveways, front doorways, and yards of businesses or houses.

Special rules apply to the video surveillance of the workplace. In general, video surveillance of an area of the workplace that is accessible and viewable by others during work hours may be done without a search warrant. Video surveillance of employee work areas that are not publicly accessible or viewable usually may not be undertaken without a search warrant. Consult with the local AUSA or appropriate DOJ attorney prior to conducting video surveillance when there is any question whether a particular area is publicly accessible.

A search warrant is required to obtain video evidence that cannot be observed from a public place with the un-aided eye. If video surveillance utilizing sense enhancing technology is contemplated, the local AUSA or appropriate DOJ attorney should be consulted prior to the using this technique.

160.6.2 Public Areas Entitled to Fourth Amendment Protection. Video surveillance into public areas, such as a rest room, where one would reasonably expect his/her actions to be private must comply with Fourth Amendment standards and may require a warrant. See Section 160.8.

160.6.3 Video Surveillance When Consenting Party is Present. SAs may observe and record (video) private meetings between an undercover officer or cooperating witness and subjects if the premises are controlled by the SA or witness.

160.6.4 Court Orders for Video Surveillance. If a court order is required due to the place to be surveilled, the pleadings are to be based on Rule 41(b) of the Federal Rules of Criminal Procedure and the All Writs Act (28 U.S.C. § 1651). The courts of appeals in six Federal circuits, while recognizing that video surveillance does not fall within the letter of Title I, require that applications to use video surveillance of suspected criminal activities meet most of the higher constitutional standards required under Title I (*e.g.*, necessity and minimization). Therefore, the application and order should be based on an affidavit that establishes probable cause to believe that evidence of a Federal crime will be obtained by the surveillance and should also include:

- A statement indicating that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or are too dangerous;

- A detailed description of the premises to be surveilled;
- The names of the persons to be surveilled, if known;
- A statement of the steps to be taken to ensure that surveillance will be minimized to effectuate only purposes for which the order is issued; and
- A statement of the duration of the order, which shall not be longer than necessary to achieve the objective of the authorization nor, in any event, longer than 30 days, measured from the date of the order (without any 10-day grace period to begin interception, but with 30-day extension periods possible).

160.6.5 Installation and Operation of Video Monitoring Equipment. DTAs are trained in the installation and operation of a wide variety of specialized video equipment. SAs should contact their DTA for assistance. Installation of pole cameras and similar specialized video systems require extensive planning and lead time. SAs should involve the DTA early in the planning process to ensure adequate technical investigative support.

160.7 Interception of Oral Communications.
When an SA wants to intercept oral communications as well as video images within the same target premises, a Title I court order is required without the consent of one of the persons. See Section 170 for additional information related to consensual monitoring. The SA may use the same affidavit to establish probable cause for the use of the microphone and the camera. Separate applications and orders, however, should be filed for each type of interception because each may be governed by a different standard, and the pleadings should reflect this difference. See Section 170 for additional information related to Title I intercepts.

160.8 Technical Surveillance and Countermeasures.
TFSD maintains an inventory of technical surveillance and countermeasures (TSCM) equipment. Only qualified personnel may operate TSCM equipment. This equipment is used to detect the presence of surreptitious surveillance devices. TSCM operations examine the integrity of telephone systems, office/home furnishings and structural elements of a facility in order to detect the presence of active/passive surveillance devices.

160.8.1 Technical Surveillance and Countermeasures Authorization. Generally, facilities subject to TSCM examination are under the control of a U.S. Government agency. On occasion, TIGTA and/or Internal Revenue Service (IRS) employees are provided workspace in taxpayers' offices while conducting audits and other activities. In such situations, a TSCM operation may be limited to the immediate interior space occupied by TIGTA/IRS personnel. The opinion of a local AUSA should be solicited if the location of the proposed TSCM is not owned or under the control of the U.S. Government. TFSD also provides TSCM services to other Treasury bureaus.

Prior to initiating a TSCM request, the SAC should consult with TIGTA Counsel, as appropriate. The Assistant Inspector General for Investigations (AIGI)-Threat, Agent Safety, and Sensitive Investigations Directorate authorizes requests for TSCM's and provides the resources necessary to accomplish a TSCM.

160.8.2 Technical Surveillance and Countermeasures Procedures. TSCM services shall be requested by the SAC through a memorandum to the appropriate AIGI. Approved requests are forwarded to the SAC-TFSD for assignment to the ASAC-Investigative Support. The ASAC-Investigative Support coordinates the TSCM operation with the requestor. The ASAC-Investigative Support is responsible for coordinating and completing all TSCM services and will ensure the proper equipment is made available and that the proper personnel are assigned to conduct the TSCM.

If a request for TSCM services involves a facility in which a computer intrusion is suspected, the ASAC-Investigative Support will coordinate with the SAC-Cybercrimes Investigation Division to assist in the TSCM operation.

Note: Care should be taken not to discuss the TSCM in proximity to the location of the proposed place to be examined since this might compromise the integrity of the TSCM.

160.9 Surveillance Platforms.
TFSD manages a fleet of surveillance platforms to support investigations. Surveillance platforms are assigned to DTAs who maintain accountability and control over the platform. Surveillance platforms are generally equipped with a variety of audio, video and communications equipment to gather evidence from a stationary location.

160.10 Control of Technical Investigative Equipment.
Only the following personnel are authorized access to technical investigative equipment:

- OI executives;
- SACs and ASACs;
- TFSD staff; and
- TSOs.

160.10.1 Inventory. Technical investigative equipment is inventoried in accordance with the annual TIGTA personal property inventory.

160.10.2 Storage and Security. Technical investigative equipment shall be stored in centralized locations to limit unauthorized access and facilitate administrative control. Lock storage areas and account for equipment at all times.

Contact TFSD for instructions and requirements for safeguarding technical investigative equipment. SAs are responsible for safeguarding technical investigative equipment issued for their use.

Contact TFSD for guidance concerning dedicated security rooms and/or alarm systems for division offices and posts-of-duty with sensitive investigative equipment or large inventories of technical equipment.

160.10.3 Locks and Security Containers. Provide combinations or keys only to those who have a need to have access to the area, room or container. Control keys and locks even when not in use.

Retain a record of each combination using Standard Form 700, *Security Containers Information*. Form 700 is a three-part form. Enter all information on Part I, separate parts and attach Part I to the inside of the container. The combination is recorded on Part II, which is placed inside Part III and sealed. Specify the classification as "unclassified" on Parts II and III unless national security information is kept in the container. The SAC-Division, or his/her designee, maintains control over Forms 700 in a safe in his/her office. The Form 700 for each division is maintained by the appropriate AIGI. The security container in which Forms 700 are kept must offer at least the same protection level as that required by the corresponding area or container that it controls.

Keep the number of duplicates to a minimum. The officials named above keep one copy of the key properly identified as to container number, location and activity with the combination records. Record all keys issued on a TIGTA Form OI 1930, *Custody Receipt for Government Property*.

160.10.4 Security During Use. Do not leave technical investigative equipment in unattended vehicles except when absolutely necessary or when removal could compromise an investigation. Only store such items in the trunk of an unattended vehicle for a short period of time. Always lock the vehicle doors.

160.10.5 Shipment. Ship all technical equipment via next day shipping, unless otherwise directed by the SAC-TFSD.

If any equipment has been lost in shipment, the shipping office must immediately:

- Process all claims for reimbursement from the overnight courier; and
- Notify the appropriate ASAC-TFSD immediately of the loss, identify the equipment and provide the air bill number, indicated on the copy.

160.11 Equipment Loans and Technical Assistance.
The SAC-TFSD is the approving authority for loans of sensitive investigative equipment to and from another law enforcement agency. The SAC-TFSD also approves each request for technical assistance to other law enforcement agencies in support of the loaning of equipment. Technical assistance is defined as instruction in the operation of the equipment and/or assistance in the actual installation of the equipment. The person

requesting a loan of equipment shall provide a letter from their agency setting forth the following:

- Operational requirement for loan;
- Duration of proposed loan; and
- Technical assistance required, if applicable.

Note: Only DTAs may provide preliminary assistance to other law enforcement agencies with regard to the basic operating features of equipment loaned. The actual operation of equipment loaned to another agency is not permitted, except as specifically authorized by the AIGI-Threat, Agent Safety, and Sensitive Investigations Directorate. Investigations in which OI is a joint participant do not require the AIGI approval for the loaning of equipment and related technical support.

Once approved, the DTA must complete TIGTA Form OI 8460, *Equipment Use Agreement and Assumption Liability*, to document all equipment loans. The SAC-TFSD must approve the loan of sensitive electronic equipment by signing the form. The authority to loan other equipment may be re-delegated.

Note: Failure to obtain approval may subject the TIGTA employee who releases the equipment to criminal and civil charges without the protection provided under the Federal Tort Claims Act.

TFSD will maintain the original TIGTA Form OI 8460. DTAs will document in the Personal Property Manager system when technical investigative equipment is loaned.

160.12 Disposal of Technical Investigative Equipment.
Technical investigative equipment will be disposed of in accordance with Federal property management regulations. See Chapter 600, Section 100, *Personal Property Management Program*.

DATE: July 1, 2020

CHAPTER 400 – INVESTIGATIONS

(400)-170 Intercept of Communications

170.1 Overview.
This Section includes the following information related to the interception of communications by the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations (OI):

- Authority
- Authorized Users
- Evidence
- Consensual Telephone Monitoring
- Record of Monitoring
- Consensual Non-Telephone Monitoring
- Title III Intercepts
- Pen Register
- Trap and Trace
- Facsimile/Computer Internet Intercepts
- Cell-Site Simulator System

170.1.1 Acronyms Table.

170.2 Authority.
The Fourth Amendment to the United States Constitution, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (also known as the Wiretap Act), as amended (18 U.S.C. § 2510, et seq.), and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801, et seq.), permit Government agents, acting with the consent of a party to a communication, to engage in warrantless monitoring of wire communications and oral, non-wire communications. The Constitution and Federal statutes permit Federal agents to engage in warrantless monitoring of oral, non-wire communications when the communicating parties have no justifiable expectation of privacy.

The United States Attorney General's Memorandum, dated May 30, 2002, "Procedures for Lawful, Warrantless Monitoring of Verbal Communications," to the heads and Inspectors General of Executive Departments and Agencies, establishes the procedures for intercepting, overhearing, transmitting, and/or recording of oral, non-wire communications, with the consent of at least one of the parties (consensual monitoring).

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. § 2510, et seq.), the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801, et seq.), and Title 18, Part I, Chapter 119, Wire and Electronic Communications Interception and Interception of Oral Communications, contain the definition, authority

and procedures for nonconsensual interceptions of wire, oral or electronic communications for law enforcement purposes.

Electronic communications are divided into the following categories:

- Communications during the transmission stage; and
- Communications in "storage" incident to transmission (historical data).

The Electronic Communications Privacy Act of 1986 establishes procedures for the collection of electronic communication transmissions. Generally, electronic communications are those which do not contain the human voice at any point during the transmission. See Title 18 U.S.C. § 2510(12) for the definition of an electronic communication. The amendments to Title 18 U.S.C § 3127 enacted in the USA Patriot Act of 2001 broadened the scope of "pen register" and "trap and trace device" to include cellular non-content electronic transmissions of dialing, routing, addressing and signaling information as transmissions governed by these statutes.

Due to the sensitive nature of the use of advanced technical investigative techniques, several of the techniques discussed in this section require appropriate legal approvals and administrative authorizations. When a case requires the use of such techniques, special agents (SA) must proceed as follows:

- **Administrative Approval:** SAs will discuss the technique with the Special Agent in Charge (SAC) or Assistant Special Agent in Charge (ASAC) and obtain appropriate approvals prior to addressing legal issues.

- **Legal Authority:** SAs must consult with the local Assistant United States Attorney (AUSA) and obtain a court order, if required. SAs will consult with TIGTA Counsel, through the Operations Division, as appropriate.

- **Technical Feasibility:** SAs will contact the Divisional Technical Agent (DTA) for technical advice and coordinate with the DTA for assistance in employing the technique upon resolution of administrative and legal issues.

Failure to obtain appropriate legal advice and authority can result in disciplinary action and/or criminal and/or civil liability.

170.3 Authorized Users.
Only technically qualified DTAs and Technical Services Officers (TSO) are authorized to use, or direct the use of, sensitive investigative technical equipment.

DTAs and TSOs, where necessary, may direct other SAs to install and operate sensitive investigative equipment, such as electronic surveillance devices, pen registers, or other covert investigative aids.

In emergencies, TIGTA managers may authorize other SAs to perform this function.

170.3.1 Prohibited Uses. Do not use, or allow the use of, technical investigative equipment without approval as described in this section.

Monitoring or recording telephone calls with mechanical, electronic or other devices is prohibited in matters other than criminal investigations.

TIGTA OI personnel, or persons acting under their direction, may not permanently install concealed microphones, recording equipment, covert video cameras, voice transmitters or similar types of equipment inside or outside any Internal Revenue Service (IRS) office. This prohibition does not extend to physical security or alarm devices used to protect IRS property or personnel from harm.

Without the prior consent of at least one of the parties to the communication (consensual monitoring), the following interceptions are not permitted:

- Telephone, including cellular and cordless conversations or other electronic signaling or data information which accompany telephone service;
- Individual and group non-telephone conversations; or
- Facsimile information.

Non-consensual monitoring of wire communications is prohibited without a **court order**, even if SAs do not intend to use the information in any way or divulge the information outside TIGTA.

SAs must obtain prior approval from a TIGTA OI management official and/or the U.S. Department of Justice (DOJ) to use mechanical, electronic, or other devices to overhear, transmit, or record any wire or non-wire communication. TIGTA OI management officials can only grant permission to SAs to intercept, record, and transmit wire and non-wire communications. Once authorization is received, SAs may allow persons working under their direction to assist.

TIGTA employees who knowingly sanction violations of monitoring procedures are subject to disciplinary action, including removal from TIGTA, and criminal or civil prosecution or both. Additionally, SAs may not be protected from state sanctions, normally afforded to Federal officials acting within the scope of their employment, if they violate the interception of communications procedures. The prohibitions and limitations in using electronic equipment apply equally to IRS personnel and/or non-employees who are acting at the direction of SAs. SAs may not use personally owned devices during their investigative activities.

170.3.2 Use on Commercial Aircraft. Generally, the operation of any two-way or broadcast-band radio equipment on commercial aircraft is prohibited to avoid interference with the aircraft's navigational equipment. This prohibition includes cellular telephones, low power surveillance transmitters, receivers and recorders. DTAs and TSOs must ensure that TIGTA personnel and cooperating persons do not operate transmitting equipment aboard aircraft during authorized consensual monitoring.

If technical investigative equipment must be used on an aircraft during flight, the DTA must contact the airline corporate security office for initial approval. Through coordination with the DTA, the SAC must submit a memorandum requesting an exemption to the airline carrier's corporate security office.

Forward a copy of the signed memorandum to the Federal Aviation Administration (FAA) and the appropriate Assistant Inspector General for Investigations (AIGI). Emergency requests for an exemption may be made by telephone or facsimile to the airline carrier and FAA. The SAC must submit a memorandum, as soon as possible, but no later than five workdays after the emergency request.

170.3.3 Uses Not Requiring Approval. SAs may use electronic or mechanical devices to overhear, transmit, or record non-wire conversations and make video recordings with the advance consent of **all** parties to the conversation, in connection with official law enforcement investigations

The use of standard two-way law enforcement portable and mobile radio equipment to facilitate communications between SAs and their offices is permitted. Special tone-only emergency tracking systems and alarm signaling devices not capable of passing any verbal communication can be used

170.4 Evidence.
The DTA, TSO, or equipment operator should immediately safeguard the recording from erasure or compromise, and mark the original recording for later identification. Working copies of the original recording should be made so the original can be entered into evidence. The DTA and/or TSO must always consider the chain of custody whenever handling evidentiary recordings. If immediate duplication is not possible, place the original recording in an evidence container and give it to the evidence custodian for processing and storage as evidence. SAs should make transcripts of audio recordings as soon as possible, based on consultation with their ASAC.

Pursuant to Title 18 U.S.C. § 2518 (8)(a), any wire, oral or electronic communication intercepted by means of a court order must be kept for at least ten years. See Section 190.

170.4.1 Audio/Video Recording Enhancements. The Forensic and Digital Science Laboratory has the equipment and expertise to enhance audio and video recordings. For enhancements of audio/video recordings, follow guidance in Section 190.

170.5 Consensual Telephone Monitoring.
Consensual telephone monitoring is the intercepting and recording of telephone conversations when one or more of the parties to the conversation consents to the lawful, warrantless interception and recording of the communication. Obtain approval from the SAC prior to monitoring any telephone calls. The approval may be made by telephone. The initial approval cannot exceed 60 days.

170.5.1 Consensual Telephone Monitoring Log. The SAC must maintain a Consensual Telephone Monitoring Log of all approvals. The log may be in hardcopy or electronic format, must be separated by fiscal year, and contain the following information:

- Case title and case number;
- Case SA, name of SA requesting permission, and the division making the request, if the request is from another Division;
- Date when 60 day monitoring begins; and
- Initials and date of the approving SAC (enter the last name of the SAC if the request is from another Division).

170.5.2 Extensions. Extensions for consensual telephone monitoring are requested in the same manner as initial requests. SACs must document the extension in the Consensual Telephone Monitoring Log. Each extension cannot exceed 60 days.

170.6 Record of Monitoring.
Use TIGTA Form OI 6171, *Record of Monitoring,* to document consensual telephone and non-telephone monitoring approvals and each monitoring conducted.

Complete TIGTA Form OI 6171 if consensual monitoring is completed for another division. After monitoring, forward the original TIGTA Form OI 6171 to the requesting SA with the original recordings of the monitored conversations.

Additionally, complete TIGTA Form OI 2028-M, *Memorandum of Interview or Activity,* to document each consensual telephone or non-telephone monitoring.

170.7 Consensual Non-Telephone Monitoring.
Consensual non-telephone monitoring is the intercepting, transmitting, and recording of oral, non-wire communications, when one or more of the parties to the conversation consents to the lawful, warrantless interception and recording of the communication.

170.7.1 Authorization for Use. The monitoring of non-telephone conversations with the consent of one party requires the advance authorization of either the Attorney General or his/her designee or a designated TIGTA management official.

The Inspector General has designated the Deputy Inspector General for Investigations (DIGI), AIGIs, and the Deputy AIGI (DAIGI) as TIGTA management officials who may authorize consensual non-telephone monitoring. This authority cannot be re-delegated. See TIGTA Delegation Order No. 22. When Attorney General approval is required, the DIGI approves the request and forwards it to the DOJ.

See Section 170.7.2.1 of this section for request procedures and circumstances requiring Attorney General approval.

In all consensual non-telephone monitoring situations, SAs must obtain advice from a DOJ trial attorney that the monitoring is legal and appropriate. SAs may obtain advice orally. DOJ trial attorneys include the following:

- United States Attorney;
- AUSA; and
- Designated DOJ attorney for a particular investigation, including Public Integrity Section attorneys.

170.7.2 Submission of TIGTA Form OI 5177. SAs must submit TIGTA Form OI 5177, *Request for Authorization to Use Electronic Equipment and Consensual Monitoring,* through the ASAC to the SAC for approval. The SAC will forward the TIGTA Form OI 5177 to the *TIGTA Inv Operations inbox as soon as the need for monitoring is known.

If consensual non-telephone monitoring is to occur within two days or less of submitting the monitoring authorization request, the SAC shall e-mail the *TIGTA Inv Operations inbox to ensure that TIGTA Counsel and a TIGTA approving official are available to review and approve the request.

For sensitive circumstances that require Attorney General approval, the TIGTA Form OI 5177 must be approved by the DIGI by forwarding the completed form to the *TIGTA Inv Operations inbox no less than 72 hours prior to the day the monitoring is scheduled to begin. Operations Division personnel will coordinate with DOJ to obtain approval.

SAs must also follow the same procedures when requesting extensions.

If the consensual non-telephone monitoring request is approved, a copy of the approved TIGTA Form OI 5177 is forwarded to the SAC, ASAC, and SA to be placed in the original case file.

170.7.3 Sensitive Circumstances Requiring Written DOJ Approval. A request for authorization to monitor an oral, non-wire communication without the consent of all parties to the communication must be approved in writing by the Director or Associate Director of the DOJ Criminal Division, Office of Enforcement Operations (OEO) when it is known that:

- The monitoring relates to an investigation of a member of Congress, a Federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;
- The monitoring relates to an investigation of the governor, lieutenant governor, or attorney general of any state or territory, or a judge or justice of the highest court of any State or territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties;
- Any party to the communication is a member of the diplomatic corps of a foreign country;
- Any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;
- The consenting or non-consenting person is in the custody of the Bureau of Prisons (BOP) or the U.S. Marshals Service (USMS); or
- The Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the U.S. Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

170.7.4 Monitoring Not Within the Scope of the Attorney General's Memorandum. Even if the interception falls within one of the sensitive circumstances listed above, the Attorney General's Memorandum does not apply to the following:

- Extraterritorial interceptions;
- Foreign intelligence interceptions, including interceptions pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801, et seq.);
- Interceptions pursuant to the court-authorization procedures of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. § 2510, et seq.);
- Routine BOP monitoring of oral communications that are not attended by a justifiable expectation of privacy;
- Interceptions of radio communications; and/or
- Interceptions of telephone communications.

170.7.5 Verbal Requests/Approval. SAs should always attempt to obtain advance written authorization prior to monitoring consensual non-telephone conversations. In exigent circumstances, the SAC can call an AIGI or the DAIGI and request verbal approval. If one of these management officials is not available, the SAC must request approval from the DIGI.

Verbal requests must include all of the information required for written requests.

E-mail TIGTA Form OI 5177 to the *TIGTA Inv Operations inbox within 24 hours after receiving verbal approval.

170.7.6 Emergency Monitoring Approval. Emergency requests requiring written DOJ approval may be made by telephone to the Director or an Associate Director of the DOJ Criminal Division, OEO or to the Assistant Attorney General, or a Deputy Assistant Attorney General of the Criminal Division, if the appropriate TIGTA official approves the monitoring. See Section 170.8.2.1 for monitoring requiring written DOJ approval.

In situations requiring written DOJ approval and one of the individuals identified in Section 170.8.6 cannot be reached, the Inspector General or his/her designee may authorize emergency consensual non-telephone monitoring. TIGTA must then notify the DOJ Criminal Division, OEO as soon as practicable, but no later than three working days after the emergency monitoring authorization. The notification must be in a memorandum. The memorandum must explain the emergency and contain a completed TIGTA Form OI 5177. Forward the memorandum to the *TIGTA Inv Operations inbox for the DIGI's approval and referral to the DOJ Criminal Division, OEO.

In situations not requiring written DOJ approval, SACs may authorize temporary emergency consensual non-telephone monitoring. They may do so only after an unsuccessful attempt to obtain advance verbal approval from the DAIGI, an AIGI, or the DIGI. The authority to grant emergency approval cannot be re-delegated. See TIGTA Delegation Order No. 22.

When SACs grant emergency approval, notify the DAIGI and/or AIGI by the next business day. They must also submit a memorandum and completed TIGTA Form OI 5177 to their respective DAIGI or AIGI by forwarding the memorandum to the *TIGTA Inv Operations inbox, within 48 hours to serve as the record of emergency authorization.

170.7.7 Authorization in Sensitive Circumstances. The following DOJ officials have authority to grant approval to engage in consensual non-telephone monitoring in the sensitive circumstances listed in Section 170.8.2.1:

- Attorney General;
- Deputy Attorney General;
- Associate Attorney General;
- Assistant Attorney General or Acting Assistant Attorney General, Criminal Division;
- Deputy Assistant Attorney General, Criminal Division; and
- Director or an Associate Director, Criminal Division, OEO.

170.7.8 Special Limitations. When a party to a conversation consent to the monitoring of his/her oral communication (consenting party), the monitoring device may be concealed on his/her person, in his/her personal effects, or in a fixed location.

TIGTA must ensure the consenting party will be present at all times when the device is operating.

170.7.9 When Written DOJ Approval is Not Required for Consensual Non-Telephone Monitoring. SAs must contact the U.S. Attorney, an AUSA, or the DOJ attorney responsible for a particular investigation prior to receiving approval for consensual non-telephone monitoring from a TIGTA management official. The U.S. Attorney, AUSA, or DOJ attorney responsible for a particular investigation must advise as to both the legality and appropriateness of the consensual non-telephone monitoring.

170.7.10 TIGTA Form OI 5177. SAs must use TIGTA Form OI 5177 to request approval for each investigation. The SAC must send a completed TIGTA Form OI 5177 to the *TIGTA Inv Operations inbox for approval.

170.7.11 Submission of New TIGTA Form OI 5177. SAs must submit a new TIGTA Form OI 5177 when any of the following circumstances exists:

- There is a new consenting party or additional consenting party;
- SAs will monitor conversations of a new subject and TIGTA has initiated an investigation on the subject; or
- Monitoring under the original authorization implicates a third party in possible criminal activities and there is no substantiated connection between the third party's activities and the subject of the investigation.

SAs do not need new approval for minor adjustments or additions to equipment described in Block #9 of TIGTA Form OI 5177.

SAs are not required to submit a new TIGTA Form OI 5177 to monitor previously unnamed third parties who appear during meetings with the subject.

170.8 Title III Intercepts.
Title III non-consensual monitoring includes the intercepting, transmitting, and/or recording of wire, oral, and electronic communications when **none** of the parties to the communication gives consent or is aware of such interception, transmission, or recording.

See Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, (18 U.S.C. § 2510, et seq.).

170.8.1 Title III Policy. The request for a Title III court order requires that SAs show the following:

- The crime is of a nature for which the use of a Title III court order is warranted;
- All other investigative steps have been exhausted without success; and
- Further investigative activities would potentially cause either harm to agents of the Government and/or cooperating individuals or would reasonably alert the target(s) of the investigation(s).

170.8.2 Title III Authorization. Non-consensual monitoring requires a Title III court order authorizing installation and use. Pursuant to 18 U.S.C. § 2518, a U.S. District Court may issue an order authorizing the use of non-consensual intercepts. The Title III court order is valid for up to 30 days. Application for a Title III court order must be authorized by one of the DOJ officials set forth in 18 U.S.C. § 2516.

See 18 U.S.C. § 2518 for additional information on applying for a Title III court order.

Generally, a court-ordered pen register should be used prior to requesting Title III authorization for non-consensual interception of telephone conversations. The pen register shows that a particular telephone is being used in the commission of a crime and serves as the basis for the Title III request. See Section 170.10 for pen register use.

The Inspector General has the authority to approve TIGTA requests to a court for authorization to use the Title III intercept technique, and the costs associated with such use. The SA must prepare a memorandum to the Inspector General requesting to use the technique.

The SAC must forward the memorandum to the *TIGTA Inv Operations inbox for review and approval by the appropriate DAIGI/AIGI, the DIGI, and the Inspector General.

170.8.3 Title III Intercept Procedures. SAs considering use of the Title III intercept technique should contact the DTA as soon as possible to discuss the technical feasibility of using this equipment. If it is determined that the technique is feasible, complete the following:

- Contact the local U.S. Attorney's Office to determine if sufficient information exists to obtain a court order for a Title III intercept;
- Prepare a detailed affidavit that contains the information identified in Section 170.9.2; and
- Coordinate DOJ reporting requirements and procedures with the local AUSA.

170.9 Pen Register.
The use of pen registers to gather evidence in criminal cases requires SAs to obtain the following:

- Legal approval by a local AUSA for a **court order,** issued pursuant to 18 U.S.C. § 3123;
- Administrative approval from the SAC to employ and fund the investigative technique; and
- Assistance of the DTA to plan, coordinate and install appropriate devices.

A pen register court order **does not** authorize the monitoring of oral communications, the interception of contents of e-mail, or call data (*e.g.,* text messages).

170.9.1 Pen Register Authorizations. A court order is required to install and use a pen register. Discuss the specific legal requirements of the proposed installation with a local AUSA prior to utilizing this technique.

Contact a local AUSA for advice and assistance concerning the level of information required to obtain a court order. Consult with the Operations Division, who will consult with TIGTA Counsel, as appropriate.

The SAC is the approving official for making application to a court for authorization to use the pen register technique and committing the resources necessary to accomplish the gathering of evidence. The SA will prepare a memorandum to the SAC outlining the proposed use of a pen register, the costs associated with installation and operation of technical equipment, and other resources required.

In urgent cases, approval to use a pen register may be made by telephone. As soon as possible after verbal approval is obtained, submit a memorandum with the information described above, to the SAC.

170.9.2 Requesting a Pen Register. SAs should consult with the DTA assigned to their division when considering a pen register. The DTA will assist the SA in gathering technical information, planning the installation of equipment, and making the appropriate contacts with the telephone company.

170.9.3 Pen Register with Subscriber Permission. A court order is generally not required when the subscriber has given permission for the installation of a pen register on his/her telephone. Complete all the requirements for requesting approval, with the exception of obtaining a court order. Document the subscriber's consent in writing and ensure that the consenting party is lawfully authorized to give consent.

170.10 Trap and Trace.
Most telephone companies have the capability to "trap and trace" a subscriber's telephone. A "trap and trace" device is used by a telephone company to discover the originating numbers of incoming calls and can also capture the e-mail addresses of individuals who send e-mails to a subscriber. This information frequently supplements data gathered by a pen register. In some instances, a "trap and trace" may eliminate the need for a register.

170.10.1 Trap and Trace Authorizations. In most instances, the use of a "trap and trace" device requires a court order authorizing its installation and use. Discuss the specific legal requirements of the proposed installation with a local AUSA prior to utilizing this technique. In addition, SAs may consult with the Operations Division, who will consult with TIGTA Counsel, as appropriate.

SAs considering the use of the “trap and trace” technique should consult with the local DTA to consider other options (*e.g.*, pen register).

See 18 U.S.C. §§ 3121 – 3123 for detailed information regarding trap and trace court orders.

The SAC is the approving official for making application to a court for authorization to use the “trap and trace” technique and committing the resources necessary to accomplish the gathering of evidence. The SA will prepare a memorandum to the SAC outlining the proposed use of the “trap and trace” technique, the costs associated with such operation, and other resources required.

The DTA will contact the local telephone security office for technical assistance and instructions.

Generally, the telephone company, once in receipt of the court order, will make arrangements to provide detailed call reports to the SA on a regular schedule. These reports should be handled as evidence and maintained in accordance with Section 190.

170.10.2 Trap and Trace with Subscriber Permission. A court order is generally not required when the subscriber has given permission to place a "trap and trace" on his/her telephone. Complete all the requirements for requesting approval, with the exception of obtaining a court order. Document the subscriber's consent in writing and ensure that the consenting party is authorized to give consent.

170.11 Facsimile/Computer Intercepts.
Non-consensual facsimile and/or computer intercepts are considered electronic communication intercepts and require a Title III court order authorizing installation and use. Electronic communications are divided into the following categories:

- Communications during the transmission stage; and
- Communications in "storage" incident to transmission, which require special handling and coordination.

Title 18 U.S.C. § 2703 contains requirements for government access to contents of or records concerning electronic communications in storage by an electronic communication service or remote computing service, such as an Internet Service Provider. Like requests for court orders involving other Title III intercepts, DOJ must review and approve applications prior to the court authorizing the Title III court order. Unlike requests for court orders involving other Title III intercepts, which must show allegations are within the offenses contained in 18 U.S.C. § 2516, facsimile and computer intercepts can be used for any Federal felony. See Section 170.9.2 for Title III authorization.

170.11.1 Facsimile/Computer Intercept Authorization. Non-consensual facsimile or computer intercepts require a court order authorizing installation and use. Discuss the specific legal requirements of the proposed installation with a local AUSA prior to utilizing this technique.

These types of intercepts are considered non-voice Title III court orders, but still require DOJ review and approval. Generally, a court-ordered pen register should be used prior to requesting Title III authorization. The pen register shows that a particular telephone line is being used in the commission of a crime and serves as a basis for the Title III court order.

The Inspector General must approve an application to a court for authorization to use the facsimile or computer intercept technique.

The SAC must forward the memorandum to the *TIGTA Inv Operations inbox for review and approval by the appropriate DAIGI/AIGI, the DIGI, and the Inspector General.

170.11.2 Facsimile/Computer Intercept Procedures. SAs considering use of the facsimile or computer intercept technique should contact the Cybercrime Investigations Division (CCID) as soon as possible to discuss the technical feasibility of using facsimile or computer intercept devices.

170.11.3 Facsimile/Computer Installation and Operation. Contact CCID to make arrangements to obtain the facsimile/computer intercept equipment and the technical assistance for installation of the device. If using a computer intercept, coordinate with the CCID for guidance.

170.11.4 Facsimile/Computer Intercept with Subscriber Permission. A court order is generally not required when the subscriber has given permission to capture his/her facsimile or computer information. Complete all the requirements for requesting approval, with the exception of obtaining a court order. Document the subscriber's consent in writing and ensure that the consenting party is lawfully authorized to give consent.

If the computer intercept meets the requirements of the computer trespass exemption in 18 U.S.C. 2511(2)(i) and subscriber permission is obtained as stated above, the procedures in Section 170.13.4.1 below must be followed.

170.11.4.1 Computer Intercept Using Trespass Exemption. When the computer intercept meets the requirements in 18 U.S.C. § 2511(2)(i), authorization to use the technique are approved by the SAC. It is recommended that the approving SAC consult with the CCID for de-confliction purposes.

The requesting SA is not required to obtain concurrence from a DOJ attorney when the computer trespass exemption applies; however, the computer intercept must meet all of the requirements in 18 U.S.C. § 2511(2)(i).

If the computer intercept meets all of the requirements as stated, the requesting SA must prepare a memorandum to the SAC. The SAC must forward the memorandum to the SAC-CCID for concurrence. If approved, the SAC must forward a copy of the signed memorandum to the DAIGI and the appropriate AIGI.

170.12 Cell-Site Simulator System.
A Cell-Site Simulator System functions by transmitting as a cell tower. In response to the signal emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the cell tower and transmit signals to the simulator that identify the device in the same way that they would with a networked tower.

170.12.1 Cell-Site Simulator Usage Authorization. SAs must be familiar with the legal and administrative considerations related to the use of cell-site simulators. Agents should always consult with an AUSA in advance of using a cell-site simulator. See Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology.

The use of a cell-site simulator is permitted only as authorized by law and policy. While past authorization to use a cell-site simulator may have been sought through use of the Pen Register Statute, as a matter of policy, law enforcement agencies must obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or the applicable state equivalent).

There are two circumstances in which this policy does not require a warrant prior to using a cell-site simulator:

- Exigent Circumstances Under the Fourth Amendment

  In exigent circumstances, cell-site simulators still require court approval in order to be lawfully deployed. An exigency that excuses the need to obtain a warrant must be determined to be objectively reasonable and may include the need to protect human life or avert serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice. In these circumstances, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.,* which ordinarily requires judicial authorization before use. In order to comply with the terms of this policy and with 18 U.S.C. § 3125, the operator must obtain agency approval and contact the duty AUSA, who will then call the DOJ Command Center to reach a supervisory attorney in the Electronic Surveillance Unit of the OEO. The government must certify that the information sought is relevant to an ongoing criminal investigation and that the subset of exigent circumstance for an emergency pen register is listed in 18 U.S.C. § 3125.

- Exceptional Circumstances Where the Law Does Not Require a Warrant

  Under limited circumstances other than exigent, the law does not require a search warrant when circumstances make obtaining a search warrant impracticable. In such cases, agents must first obtain agency executive level approval and approval from the relevant U.S. Attorney and a Criminal Division Deputy Assistant Attorney General. In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.,* which ordinarily requires judicial authorization before use and the government must certify that the information sought is relevant to an ongoing criminal investigation. In addition, if circumstances necessitate emergency pen register authority, compliance with the provisions outlined in 18 U.S.C. § 3125 is required.

The SAC is the approving official for making application to a court for authorization to use the cell-site simulator system and committing the resources necessary to accomplish the gathering of evidence. The SA will prepare a memorandum to the SAC outlining the proposed use of this system, the costs associated with installation and operation of technical equipment, and other resources required.

170.12.2 Data Collection and Disposal. When using a cell-site simulator, agents and DTAs are responsible for ensuring that law enforcement practices concerning the collection or retention of data are lawful, and appropriately respect the important privacy interests of individuals and operate in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying information. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence, the use of cell-site simulators shall include the following practices:

- When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily.
- When the equipment is used to identify an unknown cellular device, all data must be deleted as soon as the target cellular device is identified and in any event no less than once every 30 days.
- Prior to deploying a cell-site simulator for another mission, the operator must verify that the equipment has been cleared of any previous operational data.

170.12.3 Cell-Site Simulator Procedures. SAs considering the use of the cell-site simulator intercept technique should contact a DTA as soon as possible to discuss the technical feasibility of using the equipment. The DTA will facilitate the assistance of partner Federal law enforcement agencies (*e.g.*, USMS) that use the technology on a regular basis.

The ability to disclose material protected by Title 26 U.S.C. § 6103 must be considered when assistance from other Federal law enforcement agency is possible. Contact TIGTA Counsel for assistance.

170.12.4 Cell-Site Simulator Intercept with Subscriber Permission. A search warrant is generally not required when the subscriber has given permission for the capture of his/her cell phone information as long as the owner maintains control of their phone. Complete all the requirements for requesting approval, with the exception of obtaining a search warrant. Document the subscriber's consent in writing and ensure that the consenting party is authorized to give consent.

If the owner is no longer in control of their cellular telephone (*e.g.*, the cellular telephone was stolen), a search warrant may be required. The SA should contact the local AUSA for their opinion on search warrant requirements in the judicial district.

CHAPTER 400 - INVESTIGATIONS

(400)-180 Special and Undercover Operations

180.1 Overview.
This Section contains information regarding the use of special operations and undercover operations in investigations, outlined below:

180.1.1 Acronyms Table.

180.2 Classification of Investigative Operations.
Investigative operations are classified as field operations, special operations, and undercover operations. This section addresses undercover operations and special operations (UC) only. See Section 140 for field operations.

180.3 Undercover Operations.
AUC operation is an investigative technique that provides for the penetration of any criminal or potentially criminal activity, entity, or enterprise within the jurisdiction of TIGTA to obtain evidence of a criminal offense utilizing a law enforcement undercover agent (UCA) who assumes a fictitious identity or personality. Due to the increased risk

of personal injury, written approval and oversight by the Office of Investigations (OI) headquarters is required prior to conducting a UC operation. There are two classifications of UC operations - Group I and Group II.

The use of Group I and Group II undercover operations as a specialized technique will be tracked in the Criminal Results Management System (CRIMES) using Specialized Techniques Code 17 – UC Group I/II. The code must be added in CRIMES when the technique is first utilized rather than at the conclusion of the investigation.

180.3.1 Group I UC Operations. Group I UC operations require the approval of the Deputy Inspector General for Investigations (DIGI) and are defined as those UC operations where any of the following situations apply:

- the operation is anticipated to exceed 180 days;
- the operation has a projected cost of more than $20,000 in confidential expenditures;
- the operation will involve any of the sensitive circumstances in Exhibit (400)-180.3 regardless of the number of UC contacts;
- the operation involves person(s) in the Federal Witness Protection Program;
- the operation requires leasing, renting (more than 30 day increments or more than a 30 day deposit), or contracting for space, property, supplies, equipment, or facilities, outside normal government procedures;
- the operation will extend beyond the end of the fiscal year; or
- the implementation of the operation is contingent upon or requires an indemnification agreement.

Note: TIGTA can only indemnify and release parties as authorized by the Federal Tort Claims Act and otherwise consistent with Federal law.

180.3.2 Group II UC Operations. Group II UC operations require the approval of the Assistant Inspector General for Investigations (AIGI) or the Deputy Assistant Inspector General for Investigations (DAIGI) and are defined as those UC operations that:

- will not exceed 180 days without a new authorization (the DAIGI/AIGI may approve a one-time extension of 90 days);
- has a projected cost of $20,000 or less in confidential expenditures; and
- will not extend beyond the fiscal year.

Should a sensitive circumstance as defined in Exhibit (400)-180.3 occur, the Special Agent in Charge (SAC)/Director must submit a memorandum through the DAIGI or respective AIGI requesting approval from the DIGI to elevate the operation to a Group I UC operation.

180.4 Special Operations.
A special operation is a planned investigative activity in which those involved may be placed in either high-risk situations or in situations that deal with sensitive circumstances outlined in Exhibit (400)-180.3. Special operations include the following:

- execution of an arrest or search warrant involving militant, anti-government, or other known organized criminal groups;
- covert investigation conducted at an Internal Revenue Service (IRS) facility (*e.g.*, narcotics investigation utilizing a confidential source);
- systematic or structured proactive intelligence gathering initiatives, particularly those where monitoring of constitutionally protected activities are planned (*e.g.*, video or audio monitoring of or anti-government meetings), but not the routine gathering of intelligence by an agent from either local or State police agencies; and
- any investigation involving the sensitive circumstances outlined in Exhibit (400)-180.3.

Note: Covert investigations do not include bribe investigations or remittance testing. For these types of investigations, see Sections 270 and 390.

An investigation that involves any sensitive circumstance outlined in Exhibit (400)-180.3 is considered a special operation or a Group I UC operation. Special operations and Group I UC operations involving any sensitive circumstance require the approval of the DIGI.

Special operations not involving sensitive circumstances require the written approval of the DAIGI or the respective AIGI.

180.5 One-Time Assumption.
One-time assumptions are not considered field, special, or UC operations. The one-time assumption is an investigative technique that includes any of the following:

- use of temporary covers by TIGTA special agents (SAs) on surveillance or conducting routine investigative activities; or
- up to three separate substantive contacts by telephone, non-telephone, or electronic communications to individuals under investigation.

When considering a one-time assumption, the case agent will contact the National Undercover Program Manager (NUPM) to discuss, and the discussion will be documented on TIGTA Form OI 6501, *Chronological Case Worksheet* (CCW).

Use of social media during one-time assumptions is permissible; however, SAs Must coordinate with the NUPM and a UCA will be used for this purpose.

See Department of Justice (DOJ) Online Investigative Principles for Federal Law Enforcement Agents, Principle 6, Undercover Communications, for the definition of contacts made through electronic communications such as use of the Internet or facsimile. If sensitive circumstances are involved, as listed in Exhibit (400)-180.3, the case is elevated to a special operation or Group I UC operation regardless of the number of substantive contacts.

180.5.1 Approval of the One-Time Assumption. The SAC/Director has the approval authority for one-time assumptions. No more than five working days after the approval, a copy of the memorandum approving the one-time assumption, or confirming prior verbal approval, should be sent to the NUPM via encrypted e-mail. One-time assumptions are valid for 60 days. See Section 180.18.1 for extension guidelines.

180.5.2 Completion of the One-Time Assumption. At the completion of a one-time assumption, the UCA or case agent will prepare a TIGTA Form OI 2028-M, *Memorandum of Interview or Activity*, documenting the activities and results, which will be sent to the NUPM for review. The NUPM's review is required to ensure the integrity of the UC program.

The use of one-time assumption techniques as part of an investigation will be tracked in CRIMES using Specialized Techniques Code 34 – One-Time Assumption. The code must be added in CRIMES when the technique is first utilized rather than at the conclusion of the investigation.

180.6 National Undercover Program Manager.
The NUPM coordinates UC operational activities and one-time assumptions with the requesting Division. The NUPM's duties include:

- reviewing UC and special operations proposals;
- Convening the Operational Review Committee (ORC);
- attending pre-operational meetings (PROM) and other strategy sessions;
- debriefing undercover agents;
- maintaining files relating to the UC program;
- coordinating selection of UCAs;
- consulting with the ASAC-Training Team concerning basic and advanced UC training courses, as appropriate;
- controlling UC Social Security numbers (SSNs) and maintaining liaison with the Social Security Administration (SSA);
- maintaining an inventory of UC resources;
- conducting on-site reviews of all Group I UC operations; and
- conducting on-site reviews of special and Group II UC operations selected by the DAIGI/AIGI or the DIGI.

The NUPM will review all Group I UC operations every 120 days. The NUPM may also review any Group II UC operation at the direction of the DAIGI or respective AIGI. The NUPM's review will be conducted on-site and will consist of a review of the case file, the UC operation file, confidential expenditures, and Standard Form 1164, *Claims for Reimbursement for Expenditures on Official Business*. The NUPM will also interview the ASAC/AD, case agent, contact agent, and UCA. The NUPM's review will be forwarded through supervisory channels to the DAIGI or respective AIGI, who will discuss the results with the SAC/Director.

180.6.1 Undercover Resources Inventory. The NUPM maintains a UC resources inventory that might be useful to the UCA. The UC resources inventory contains items that could help project a certain image, or support a UCA's cover story and backstopping.

180.6.2 Undercover Resources Inventory Audit. The NUPM, along with a witness, shall conduct an annual audit of the UC resources inventory. This audit will be completed by January 31. The audit will include core audit findings, other audit findings, recommendations, if any, and reference materials.

The core audit criteria will include:

- an accounting and location of all items in the TIGTA UC resources inventory;
- a description of all items added to and removed from the UC resources inventory since the previous audit; and
- a description of all items in the UC resources inventory that are currently assigned to TIGTA divisions for operational or other purposes.

The audit will be documented with a memorandum and signed by both the NUPM and a witness before it is forwarded to the NUPM's immediate supervisor for review. A UC resource items inventory spreadsheet and any other pertinent information will be attached to the memorandum.

180.7 Operational Review Committee.
The ORC is a group of individuals convened to review all special operations and UC operations proposals. The ORC provides guidance on technical and legal matters, and submits a recommendation to the appropriate authority for approval or disapproval of the UC investigative technique. See Exhibit (400)-180.5 for the members of the ORC for each type of operation.

Any sensitive investigative matter, including those involving confidential sources (CS), cooperating witnesses, and cooperating subjects, may be referred to the ORC for advice, recommendation, or comment by the DAIGI or respective AIGI regardless of whether a UC operation is involved. Due to their sensitive nature, ORC deliberations shall be kept confidential and disclosures of such deliberations shall be made only after

careful deliberation by the ORC and the requesting DAIGI/AIGI. See Section 150 for information related to confidential sources.

180.8 Initiating Special or Undercover Operations.
All requests for authorization to initiate a special operation or a UC operation must be made by the SAC in a proposal memorandum and sent to the NUPM who will forward the proposal to the appropriate reviewing official. Proposals should be submitted as soon as possible, but not less than two weeks prior to beginning the operation.

180.8.1 Proposal Memorandum. The NUPM will review the proposal memorandum to ensure the required information is addressed (See TIGTA Form OI 7523, *Undercover Operation Review Checklist*) prior to convening the ORC. The proposal memorandum must address the criteria listed below (See Exhibit (400)–180.4):

- case title, case number, and a cryptonym;
- reason for activity;
- source of the allegation;
- violation(s);
- UC or special operation goal/desired outcome;
- proposed operation;
- danger/contingency plans - see TIGTA Form OI 7503 and TIGTA Form OI 7504 for examples;
- description and location of audio and video devices/equipment;
- counter-surveillance;
- location of operation;
- duration and dates;
- identification of targets;
- prosecutor approval;
- criminal/IRS record checks - see Chapter 700, Chief Counsel, Section 50.1 for a complete discussion of Internal Revenue Code (I.R.C.) § 6103 and the authority to access tax returns and return information;
- potential for criminal activity;
- sensitive circumstances - describe any sensitive circumstances as defined in Exhibit (400)-180.3 that are involved or anticipated. Note: Treasury guidelines for determining sensitive circumstances only address activities of government employees. However, under TIGTA policy, activities of a CS that would otherwise constitute sensitive circumstances under Treasury guidelines will be included for that determination;
- SSN(s) of subjects;
- budget (accounting for confidential, non-confidential and recoverable funds);
- other participating agencies;
- core participants;
- pre-operational meeting date; and

- CS(s).

180.8.2 Routing the Proposal Memorandum. The NUPM will route the proposal memorandum to the appropriate reviewing official.

Proposal:	**Routing:**
Group I UC Operations and Special Operations Involving Sensitive Circumstances from Field Divisions	DAIGI-Field Operations; AIGI-Field Operations; and DIGI
Group II UC Operations from Field Divisions	DAIGI-Field Operations; or AIGI-Field Operations
Group I UC Operations and Special Operations Involving Sensitive Circumstances from Headquarters Divisions	AIGI of the appropriate Directorate; and DIGI
Group II UC Operations from Headquarters Divisions	AIGI of the appropriate Directorate;
One-time assumptions	SAC

180.9 Evaluation of the Proposal.
The ORC meets within 10 working days, if possible, of receipt of the proposal memorandum to review and evaluate the request. The SAC/Director, ASAC/AD, or case agent are required to participate in the ORC meeting as advocates for the proposal. The United States Attorney, or any member of his/her staff, may also attend the meeting.

The ORC will examine the proposal to determine whether adequate measures have been taken to minimize the occurrence of sensitive circumstances and to reduce the risk of harm and intrusion created by such circumstances. An approval recommendation shall include a brief written statement explaining why the operation merits approval in light of the anticipated occurrence of sensitive circumstances.

The ORC's recommendation contains technical and legal advice, improvements and modifications, and an approval or disapproval recommendation. The NUPM will prepare a memorandum for the appropriate approving official, which will include an approval/disapproval section for Group I/Group II UC proposals and special operations proposals. The ORC will only make a recommendation for approval or disapproval of a UC operation upon reaching a majority opinion by the participating members of the ORC. Minority dissenting opinions by any participating members of the ORC will be noted in the memorandum forwarded to the appropriate approval authority.

In Group I UC operations and special operations involving sensitive circumstances, TIGTA has the final decision authority on operational matters, such as investigative techniques and resource allocation. However, if the DOJ representative does not join in

a recommendation for approval of a proposed operation because of ethical or prosecutive considerations, the DOJ representative shall promptly advise the Assistant Attorney General for the Criminal Division and the DAIGI or respective AIGI shall promptly notify the DIGI. No further action shall be taken on the proposal until the Assistant Attorney General consults with the DIGI for resolution.

180.10 Approval Authority.
The appropriate approval authority will review each proposal for mission-related cost/benefit considerations. Where applicable, the approval authority will also review the ORC's written recommendation regarding the proposal. See Exhibit (400)-180.5 for the approval authority for each type of operation.

As part of the review, the approval authority will consider the risk of:

- harm to private individuals or UCAs;
- financial loss to private individuals and businesses;
- damage, liability, or other loss to the government;
- harm to reputation;
- harm to privileged or confidential relationships; and
- invasion of privacy.

The approval authority will also consider the suitability of UCAs or cooperating individuals participating in the UC operation. For a UC operation involving the subject(s) engaging in illegal activity (see Section 180.14.4), the approval authority will consider the following factors:

- the UC operation will reasonably obtain evidence to enhance prosecution of illegal acts;
- the subjects are aware of the illegal nature of their acts; and,
- the subjects are predisposed to engage in illegal acts prior to any government inducement.

The approval authority should obtain appropriate legal opinions to resolve any unsettled legal questions concerning authority for the proposed UC operation or its conduct.

If the approval authority determines that use of the UC investigative technique is justified, the proposal memorandum will be approved and returned to the requester.

180.10.1 OI Executive Oversight. OI Executives ensure consideration is given to safeguarding the integrity of the agency, and a nexus to OI's mission in special and UC operations. OI Executives are the final approval authorities for special and UC operations.

180.11 Duration of Authorization.
A UC operation should not continue longer than is necessary to achieve the objective. For the purpose of administering a UC operation (*e.g.*, length of time before an extension is required, reporting requirements), the operation is considered to be active on the date the appropriate approval authority authorizes the operation.

180.11.1 Initiating or Extending a UC Operation on an Interim Basis. An operation which requires review by the ORC may be initiated or extended on an interim basis by the appropriate approval authority in the event of exigent circumstances for a period not to exceed 30 days. In the case of an initial authorization, budget enhancement, or change in focus, the interim authorization must be reviewed by the ORC at the first available opportunity. The ORC, upon review of the initial authorization, budget enhancement, or change in focus, will make a recommendation to the appropriate approval authority.

180.11.2 Emergency Authorization. The SAC/Director may authorize an interim UC operation, or the extension of a one-time assumption (see Section 180.5 and Section 180.10.1 for further information about the one-time assumption) if the SAC concludes that any of the following situations exist:

- protect life or property;
- apprehend or identify a fleeing offender;
- prevent the hiding or destruction of essential evidence; or
- avoid other grave harm.

Before providing authorization in these situations, the SAC/Director will attempt to consult by telephone with the Federal prosecutor and the DAIGI or respective AIGI and/or the DIGI as appropriate. The SAC/Director's authority to provide emergency authorization as stated in this section may not be delegated.

180.11.2.1 Notification of the Emergency Authorization. The SAC/Director authorizing the emergency interim UC operation will make an immediate verbal notification through the DAIGI or respective AIGI to the DIGI after the operation has been initiated, extended or renewed. The SAC/Director will follow up with a written proposal within 48 hours by encrypted e-mail through the DAIGI or respective AIGI to the DIGI for approval, with a copy to the NUPM. In addition to the proposal memorandum criteria outlined in Exhibit (400)–180.4, the SAC/Director must include a written description of the emergency situation. Upon receiving notification of an emergency authorization, the NUPM will convene the ORC. The ORC will review the proposal to identify any concerns with the written application, and will forward the results of their review to the appropriate AIGI, who will inform the DIGI.

180.12 Transmitting Sensitive Information.

All information related to special operations, UC operations, and one-time assumptions should be considered Controlled Unclassified Information (CUI) and protected from unauthorized disclosure.

Information transmitted electronically should be sent by encrypted e-mail. When transmitting hard copies, follow guidance outlined in Chapter (600)-40.2.2.3, *Packaging and Transmittal of Evidence and Sensitive Items*. If the security envelope is torn or opened, establish whether the contents may have been compromised and notify the case agent's ASAC/AD and SAC/Director for appropriate action.

180.13 Preparation for the Undercover Operation.
The SAC/Director or ASAC/AD shall discuss personal and professional conduct expectations with the UCA prior to his/her participation in an investigation. The discussion should include TIGTA's policy on alcohol consumption, government-owned vehicles, the use of government-owned or leased property, and firearms. Also, if TIGTA learns that persons under investigation intend to commit a violent crime, any UCA used in connection with the investigation shall be instructed to discourage the violence. The SAC/Director or ASAC/AD shall document this discussion in the case file.

The SAC/Director or ASAC/AD shall discuss with each UCA any of the sensitive circumstances, specified in Exhibit (400)-180.3, that are reasonably likely to occur. In addition, the SAC/Director or ASAC/AD must counsel each UCA that they will not:

- Participate in any act of violence;
- Initiate or instigate any plan to commit criminal acts;
- Use unlawful investigative techniques to obtain information or evidence;
- Engage in any conduct that would violate restrictions on investigative techniques, U.S. Department of the Treasury or TIGTA procedures and policies, including sexual or intimate relations/contact with the subjects, potential subjects, or witnesses of the investigation; or
- Participate in any illegal activity not authorized under these guidelines, except in an emergency situation.

The case agent will review conduct expectations with each individual cooperating in the UC operation.

180.13.1 Undercover Firearms. UCAs are issued a TIGTA-purchased UC firearm and are authorized to carry the firearm as a secondary weapon, and after duty hours, if they are currently qualified with the firearm. Additional UC firearms are available for issuance by the National Firearms, Agent Safety, and Training Coordinator in special circumstances. For more information concerning UC firearms, see Section 130 of this chapter.

180.13.2 Pre-Operational Meeting. The PROM is held before conducting any UC contacts to familiarize all participants with the case objectives and goals, resolve problems, and allow for changes. When practical, the case agent schedules the PROM at least two weeks prior to the start of the operation and arranges for participation of all required personnel identified in the PROM Checklist. See TIGTA Form OI 7521, *Pre-Operational Meeting Checklist*.

The case agent must use the PROM Checklist to address all pertinent items. A copy of the checklist will be provided to all PROM attendees.

Note: If a new UCA is introduced into an ongoing UC operation, another operational meeting following the PROM procedures must be held.

180.14 Monitoring and Controlling Undercover Operations.
The SAC/Director and ASAC/AD overseeing the UC operation are responsible for monitoring and controlling the undercover activities throughout the duration of the operation to ensure proper controls are in place and to ensure that any problems identified during the course of the operation are brought to the appropriate officials' attention.

180.14.1 SAC/Director Responsibilities. The SAC/Director overseeing the undercover operation must review all UC activity each month. The review includes:

- Confidential expenditures;
- Non-confidential expenses;
- Investigative reports; and
- Progress toward UC objectives.

To complete the review, the SAC/Director may need to contact the ASAC/AD, case agent, or contact agent to ensure proper controls are in place. The SAC/Director will make an annotation on TIGTA Form OI 7520, *Undercover Operations Status Report*, that a review was conducted. Problems identified during a review of the UC operation will be brought to the immediate attention of the NUPM and the DAIGI or respective AIGI.

Throughout the course of any UC operation, the case agent will consult periodically with the U.S. Attorney's Office concerning the plans, tactics, and anticipated problems of the operation.

180.14.2 ASAC/AD Responsibilities. The ASAC/AD overseeing the UC operation shall complete a monthly review of the activities of the UCA and others participating in the UC operation. The review should include any proposed or reasonably foreseeable activities for the remainder of the investigation. Any findings of impermissible conduct shall be discussed with the individual, and promptly reported to the SAC/Director

responsible for the UC operation. The UCA's ASAC/AD and SAC, if the UCA is from another division, will also be apprised of the impermissible conduct.

180.14.3 Reporting Findings of Impermissible Conduct. The SAC/Director overseeing the UC operation will report the findings to the NUPM and the DAIGI or respective AIGI. The DAIGI or AIGI will make a determination as to whether the UCA should continue his or her participation in the investigation. Whenever it is anticipated that events in a UC operation could present serious legal, ethical, prosecutive or other policy issues, the case agent will promptly notify the ASAC/AD, the SAC/Director and the NUPM. The SAC/Director will also advise and consult with the DAIGI or respective AIGI.

180.14.4 Illegal Activity. A UCA or CS shall not engage, except in accordance with the following instructions, in any activities that constitute a crime under Federal or State law. For purposes of this policy, such activity is referred to as "otherwise illegal activity."

A UCA or CS will not:

- Participate in any act of violence except in self-defense;
- Initiate or instigate any plan to commit criminal acts; or
- Use unlawful investigative techniques to obtain information or evidence for TIGTA, such as illegal wiretapping, illegal mail openings, breaking and entering, or trespass amounting to an illegal search.

180.14.4.1 Approval for Illegal Activity. No official shall recommend or approve a UCA's participation in otherwise illegal activity unless the participation is justified in order to do one of the following:

- Obtain information or evidence necessary for prosecutive purposes not reasonably available without participation in the otherwise illegal activity;
- Establish and maintain credibility or cover with persons associated with the criminal activity under investigation; and
- Prevent death or serious bodily injury.

If it becomes necessary to participate in otherwise illegal activity that was not foreseen, a UCA should make every effort to consult with the SAC/Director. For otherwise illegal activity that is a felony or a serious misdemeanor, the SAC can provide emergency authorization. If consultation with the SAC/Director is impossible and there is an immediate and grave threat to life or physical safety, a UCA may participate in the otherwise illegal activity, so long as he/she does not take part in and makes every effort to prevent any act of violence. This includes the destruction of property through arson or bombing.

The UCA will prepare a report to the SAC/Director as soon as possible after any participation in any illegal activities. The SAC/Director will submit a full report to the DIGI through the DAIGI or respective AIGI with a copy to the NUPM.

If a serious incident or act of violence should occur in the course of criminal activity and a UCA or cooperating individual has participated in any fashion in the criminal activity, the SAC/Director will immediately inform the DIGI and the appropriate Assistant U.S. Attorney (AUSA), along with the DAIGI or respective AIGI. The DIGI will promptly inform the Assistant Attorney General in charge of the Criminal Division, DOJ.

180.14.4.2 Creation of Opportunities for Illegal Activity. TIGTA may create the opportunity for an individual to engage in illegal activity that he/she is predisposed to do. Avoid entrapment, which is defined as the act of a law enforcement officer (LEO), or a person acting under the direction of, or in cooperation with the LEO, to induce an individual to commit a crime that he/she did not contemplate and would otherwise be unlikely to commit, for the purpose of criminal prosecution of the individual.

Approving officials will not approve a UC operation designed to create an opportunity for illegal activity by others unless they have determined that either:

- There is a reasonable indication that the subject is engaging, has engaged, or is likely to engage in illegal activity of a similar type; or
- The opportunity for illegal activity has been structured so that there is reason to believe that persons drawn to the opportunity, or brought to it, are predisposed to engage in the illegal activity.

180.14.5 Self Defense by the Undercover Agent. Nothing in these guidelines prohibits a UCA from taking reasonable self-defense measures to protect his/her own life or the lives of others. Report such measures to the NUPM, SAC/Director, and the DAIGI or respective AIGI, the appropriate U.S. Attorney's Office, and the DIGI, who will inform the Assistant Attorney General for the Criminal Division as soon as possible.

180.15 Undercover Finances.
UC earnings, expenditures, bank accounts, and credit card accounts require special handling. See also Chapter 600, Section 50.9 for more information about expenditures and bank accounts (imprest fund).

180.15.1 Undercover Assignment Earnings. The UCA is responsible for the proper accounting and disposition of earnings from all sources associated with the UC assignment. If the assignment involves UC employment with the IRS, obtain assistance and procedural advice from TIGTA headquarters. If the assignment involves a cooperative UC employment with a non-Federal institution, make arrangements with that organization for disposition of any earnings by returning them to the organization that furnishes the cover employment. If the assignment involves a covert UC

employment (*i.e.*, employment of the UCA in which the employer is not aware of the UCA's true identity, *etc.*), proceed as follows:

- the UCA submits to the contact agent a monthly statement of such earnings, with a remittance of the earnings in the form of a cashier's check or money order payable to TIGTA;
- the contact agent will prepare a transmittal memorandum for signature by their SAC/Director to the U.S. Department of the Treasury, Bureau of the Fiscal Service (BFS), requesting that a courtesy deposit be made on behalf of TIGTA, showing Agency Locator Code (ALC) 20040001. The funds should be allocated to the Miscellaneous Receipt Account TGT1099GRXXXXXX (Fines, Penalties and Forfeitures Not Otherwise Classified). The memorandum should also request that BFS provide the SAC/Director with the deposit ticket with a copy sent to the TIGTA Assistant Director Finance, Office of Mission Support; and
- the SAC/Director will be responsible for ensuring a Document Transmittal form (IRS Form 3210), is prepared.

Send the transmittal document, memorandum, and the cashier's check or money order, via registered mail to:

Fiscal Accounting
Attention: Accounts Receivable
Avery Street A3-G
Bureau of the Fiscal Service
P.O. Box 1328
Parkersburg, WV 26106-1328

The contact agent will retain the deposit ticket, a copy of the memorandum to BFS, a copy of the transmittal document and the UCA's monthly statement of earnings in the investigative case file.

180.15.2 Undercover Expenditures. Expenditures incurred by a UCA cannot be offset against the UCA's cover employment income. UCAs will submit monthly reimbursement claims for expenditures incurred in connection with the UC assignment to the specified imprest fund account via Standard Form 1164. Each UCA is required to submit documentation of expenses to the extent that obtaining such documentation would not jeopardize his/her security. UCAs must provide receipts or a memorandum explaining why no receipts are available for all those transactions where receipts would be expected. Claims for travel expenses and per diem incurred while the UCA is not traveling in his/her cover identity will be reimbursed using the electronic travel voucher system.

180.15.3 Checks. TIGTA may receive negotiable checks by:

- filing fictitious taxpayer returns which generate refunds;
- receiving salaries during UC employment;
- requesting lump sum moneys after completing UC employment; and
- applying for Federal, State, and local tax refunds after completing UC employment assignments or disposing of SSNs.

Note: Negotiable checks may not be obtained through processes such as direct deposit. The checks must be physically retrieved.

UC operative checks received as salaries or refunds received by contact agents must be copied and cashed as soon as practical. Neither UCAs nor contact agents should sign checks until they are ready to be cashed. UCAs should give the cash, check copy, and any earnings statement to the case agent or contact agent.

Deposits may be by money order or check, as long as they are not traceable to the UCA or contact agent. Keep copies of endorsed checks, deposit tickets, original earnings statements, and other documents in the SSN file. In ongoing UC cases, they should be kept with the case file and then transferred to the SSN file when the UC activity is completed.

Make deposits each time a UCA or contact agent receives a check. Some situations require latitude and may result in check cashing delays. In those instances, the UCA should provide the contact/case agents with the checks for safekeeping. Delayed deposits must be made as soon as practicable. The reason for any check cashing delays should be noted in the case file.

Upon completion of a UC assignment, or disposal of an SSN, the case agent or contact agent should ensure lump sum payments, and any Federal, State or local tax refunds are retrieved. The case agent should have the UCA apply for these moneys, then follow deposit procedures. Place copies of tax returns, letters, or forms for lump sum payments, checks, deposit tickets, etc., in the fictitious SSN file maintained by each division.

A fictitious tax account may not carry a credit balance from year to year. Filing returns on which tax is owed, a refund is due, or no tax is owed/no refund due eliminates this condition. A balance may also be applied as payment to the next year's return. A credit balance may be kept for investigative purposes if authorized in advance by the UCA’s SAC/Director

180.15.4 FICA/Withholding. TIGTA is responsible for reporting Federal Insurance and Contribution Act (FICA) and Self Employed (SE) postings to the Social Security

Administration (SSA). Postings occur when tax returns are filed or during an UC assignment in which the UCA is paid a salary.

By January 31st of each year, the NUPM will request from each Division the FICA/SE postings for each assigned fictitious SSN. The annual SAC Certification for Confidential Sources and Fictitious Identities shall include the FICA/SE postings for the previous calendar year. The SAC/Director shall respond by February 28th of each year with a memorandum detailing the FICA/SE postings for the previous calendar year. The NUPM notifies the SSA of the postings upon receipt of the FICA/SE information. TIGTA reports FICA/SE taxes only for SSNs, on hand and disposed of, that have not been previously reported to the SSA.

180.15.5 Credit Cards and Bank Accounts. Requests for creating fictitious credit histories by the credit reporting agencies must be made by the NUPM. UCAs, through the NUPM, will have the opportunity to obtain credit cards and open bank accounts to enhance their UC identities and establish credit histories.

The SAC/Director must keep a list of credit cards and bank accounts for each fictitious SSN controlled by his/her division. It should include the SSN, type of account, account number and expiration date as shown in Exhibit (400)-180.1. Credit cards and checkbooks must be kept in a locked container.

UCAs may buy items that can be used in the UC program to help build financial histories. Items may be purchased by UC credit card, check, or cash. The SAC/Director must pre-approve, in writing, all purchases. Payment must be made from confidential funds using a Standard Form 1164, Claim for Reimbursement for Expenditures on Official Business, with the receipt attached.

UCAs may also build financial histories by purchasing personal items. The SAC/Director must pre-approve, in writing, all purchases. UCAs may use their UC credit cards to make personal purchases, pay the credit card statement with personal funds, and will not make claims for reimbursement. UCAs must make timely payments, unless making the late payment is approved in writing by the SAC/Director for the purpose of intentionally establishing a “bad” credit history.

180.16 Reporting Undercover Activity.
The case agent must complete TIGTA Form OI 7520, *Undercover Operations Status Report*, monthly and forward it to the SAC/Director. After review and approval, the SAC/Director will forward the report, via encrypted e-mail, to the NUPM by the 10th of each month. The NUPM will review and provide the report to the DAIGI or appropriate AIGI.The case agent must maintain a monthly report of expenditures, confidential and other, using Microsoft Excel. The case agent will embed the spreadsheet of monthly expenditures into the bottom of the monthly report.

The case agent must submit a final Undercover Operations Status Report to the SAC/Director within 10 days following any of the following events: the completion of the UC operation, a determination that no further UC contacts will be made, the duration authorized to conduct the UC operation expires, or a final UC contact. UC contact means by way of Internet, telephone calls, and/or personal meetings involving use of the fictitious identities. Indicate "FINAL" in the first block titled "Report for (Month/Year)." After review and approval, the SAC/Director will forward the report to the NUPM via encrypted e-mail. Upon receipt, the NUPM will review and forward to the DAIGI or appropriate AIGI who will review and forward the report to the DIGI. The report must include, but is not limited to:

- the date of the last UC contact;
- whether the UC objectives were met (if not, state why not);
- the performance of the UCA;
- the number of cases initiated as a result of the operation;
- total cost, broken down into major cost categories such as travel, per diem, confidential expenses, non-confidential expenses, etc. Attach a copy of the final report of expenditures which separates the costs into confidential, non-confidential and recoverable funds categories;
- number of persons arrested or indicted, and the applicable statutes;
- seizures of property, money, contraband; and
- significant or unusual events or problems.

The identity of a UCA will not be documented in any investigative reports, forms, or in CRIMES. The UCA will be identified as a TIGTA UCA.

180.17 Referral Procedures.
Before referring any criminal violations to State or local prosecutors, approval must be obtained by TIGTA's Office of Chief Counsel.

Information obtained in a UC operation that falls within another agency's jurisdiction will be forwarded to TIGTA's Office of Chief Counsel for a determination whether or not the information may be provided to the appropriate agency. If disclosure is not desired, the SAC/Director should submit a memorandum of justification to the DIGI through the DAIGI or respective AIGI. The DIGI will discuss the matter with DOJ, as appropriate, prior to making a decision.

180.17.1 Release of Undercover Identity. The disclosure of the UCA's fictitious identity in an investigative report may be approved by the NUPM, with concurrence from the SAC Criminal Intelligence and Counterterrorism, on a case-by-case basis. The approval will be documented on the CCW.

Upon any inadvertent disclosure of the UCA's fictitious or true identity, the case agent must notify his/her ASAC/AD and SAC/Director immediately. The case agent will follow up with a memorandum to the SAC detailing the circumstances relevant to the inadvertent disclosure of the UCA's fictitious or true identity. The SAC must notify the DAIGI or respective AIGI and forward a copy of the memorandum, via encrypted e-mail, to the NUPM. The NUPM, the DAIGI/AIGI, along with the UCA, ASAC/AD and the SAC/Director responsible for the operation, will evaluate the circumstances and make a determination regarding continued use of the UC identity by following procedures regarding compromised fictitious identities.

Note: Upon request, the true identity of a UCA may be disclosed to the prosecuting attorney or to the court.

180.18 Extensions.
If there is a significant change in either the UC mission or proposed operation, the matter must be reviewed by the NUPM to determine whether a new authorization is necessary. A request to extend a UC operation requires a memorandum:

- for Group I Operations: From the SAC through the DAIGI or respective AIGI to the DIGI; or
- for Group II Operations: From the SAC to the DAIGI or respective AIGI.

The memorandum should describe the results obtained from the operation or explain any failure to obtain significant results. If sensitive circumstances are involved, a letter should be attached from the appropriate Federal prosecutor favoring the extension.

Send the memorandum and the letter from the Federal prosecutor to the NUPM. The NUPM will prepare a recommendation memorandum with an approval, disapproval, and date section for the appropriate approval authority.

Note: Group II UC operations may not be extended beyond 270 days. For example, if a Group II UC operation is approved for 180 days, it may be extended under a new authorization an additional 90 days for a total of 270 days. If the UC operation must continue beyond a total of 270 days or has a projected cost of over $20,000, the operation must be elevated to a Group I UC operation.

180.18.1 Request to Extend a One-Time Assumption. The respective DAIGI/AIGI may extend, on a case-by-case basis, the one-time assumption an additional 60 days, and/or extend the three substantive contacts limit by telephone, non-telephone, or electronic communications, without upgrading the case to a Group II UC operation. The SAC/Director should forward an extension request, specifying why the operation should not be upgraded, to the NUPM stating the need for the extension. The NUPM will present the request to the respective DAIGI/AIGI and notify the SAC/Director of the decision. However, if the SAC/Director concludes that an emergency situation exists

that makes this procedure too lengthy, the SAC/Director may authorize an interim/emergency extension of the one-time assumption. The SAC/Director will contact the respective DAIGI/AIGI for guidance as soon as practicable.

180.19 Undercover Cadre Program.
The Undercover Cadre Program (UCCP) is designed to identify, train, and equip SAs who have the desire to become UCAs within OI. The goal of the UCCP is to have qualified UCAs available to work in an undercover capacity throughout TIGTA. To be considered for the UCCP, agents must:

- Have three years criminal investigator experience with TIGTA, or another Federal, State, or local law enforcement agency (experience, as a cooperative education student/employee does not qualify), or possess special skills needed by the UCCP; and
- Voluntarily apply;
- Have the concurrence of their first and second line supervisor;
- Complete a UCCP application;
- Complete a psychological assessment; and
- Successfully complete a UC training program.

180.19.1 Acceptance into the Undercover Cadre Program. TIGTA uses an application process for the UCCP to provide an efficient method for completion, submission, and review of the applications. The applications will be processed utilizing a designated timetable, which will be stated in a DIGI UCCP solicitation memorandum issued to all SAs. Any SA interested in being part of the UCCP should discuss it with their ASAC/AD and complete the application provided in the DIGI solicitation memorandum. The ASAC/AD and SAC/Director will review the applications to certify that the applicant is ready to be a UCCP candidate and forward it to the NUPM for consideration. The applications will be reviewed and selections will be made.

During the training phase, the NUPM and other agents experienced in UC operations will evaluate the UCCP candidates in class, during practical exercises, and in structured social environments. Upon completion of the training, a decision will be made by OI senior management, in consultation with the NUPM, whether to invite each candidate who successfully completed the training to become a member of the UCCP. Successful completion of UC training does not guarantee that the candidate will become a UCCP UCA.

180.19.2 Undercover Cadre Status. UCA’s are divided into two statuses: active and inactive.

180.19.2.1 Active Status. Active UCAs are those who have obtained a fictitious SSN, a driver's license, and have current backstopping. Active UCAs will receive primary consideration for UC assignments and additional training.

180.19.2.2 Inactive Status. Inactive UCAs are those who meet any of the following criteria:

- have not obtained an SSN and license; or
- have the SSN and license, but request to be placed in inactive status.

Inactive UCAs are selected for assignments only when active UCAs are unavailable or unsuitable.

180.19.3 Undercover Training. The NUPM, in conjunction with the ASAC-Training Team, coordinates the training of UCAs.

180.19.4 Selection of an Undercover Agent for Assignment. Undercover agent (UCA) refers to any TIGTA SA or LEO of a Federal, State, or local law enforcement agency working under the direction and control of TIGTA in a particular investigation, whose relationship with TIGTA is concealed from third parties in the course of an investigative operation by the maintenance of a cover or alias identity. A UCA does not include Confidential Sources, either paid or unpaid, who may be providing information to a TIGTA agent (See Section 150).

Except in exigent circumstances, only UCAs will be used in UC operations.

Non-cadre operatives may only be used when no UCA is available or suitable. Non-UCA, whether TIGTA SAs or other law enforcement personnel, are used only with the advance written permission of the appropriate AIGI. The request is routed through the NUPM and will explain why the individual is desired and what training qualifies them for the assignment. When using a UCA from another law enforcement agency, identify the department and LEO's position. The case agent must submit a separate request for each non-UCA used.

Non-UCAs who are not employees of TIGTA or the IRS shall complete a statement of non-disclosure advising that they are aware of the requirements of IRC § 6103 prior to commencement of the operation.

180.19.4.1 Selection Process. The process for selecting a UCA for participation in a UC operation is:

1) The case agent, ASAC/AD, or SAC/Director contacts the NUPM as soon as a UCA is needed to discuss the profile traits of the desired UCA. The requester should advise the NUPM if a specific UCA is preferred.

2) The NUPM contacts prospective UCAs to determine their availability and interest in the assignment, and conducts the appropriate vetting to determine their suitability for all aspects of the operation and subsequent testimony.

3) The NUPM contacts the ASAC/AD, or SAC/Director, of the UCA who is preliminarily identified to participate in the operation to discuss the availability of the individual.

If a UCA repeatedly refuses UC assignments, they may be removed from the UCCP.

180.19.5 Preventing Recognition of the UCA. UCAs and case agents should discuss the level of the UCA's exposure (prior and planned) to IRS employees during investigations, speeches, or presentations, photographs in IRS or other publications, and through other mediums such as the Internet. Such exposure might lead to the UCA being recognized as a SA. This discussion should take place prior to the PROM and includes:

- the length of time between the event and the assignment;
- whether there was/will be local or nationwide attendance by IRS employees or anyone, including the target, who may recognize the UCA as a LEO; and
- strategic planning to minimize the potential of being recognized.

UCAs should consider the negative impact of:

- attending conferences where IRS employees will be present;
- giving presentations to IRS groups;
- being photographed for publications; and
- maintaining a presence on the Internet (*e.g.*, Facebook, Instagram, Twitter, LinkedIn, etc.).

UCAs attending events that are not related to their UC assignment during an operation should remain as inconspicuous as possible.

180.20 Contact Agent.
A contact agent is a designated SA, who should be a member of the UCCP, who provides administrative and investigative support to the UCA during an operation. The NUPM will select a contact agent in consult with the case agent and ASAC/AD. The contact agent should be located at, or as close as possible to, the operational site.

180.20.1 Contact Agent Duties. The principal duties of the contact agent are to:

- contact the UCA daily for safety and support;
- receive daily activity and financial reports from the UCA, if practical;

- provide assistance in the preparation of reimbursement claims;
- transmit instructions and information to the UCA;
- ensure that TIGTA's objectives are being carried out by the UCA;
- attend to the security and safety of the UCA; and
- provide immediate assistance in any emergency.

Based on information furnished by the UCA, the contact agent may:

- prepare reimbursement claims for funds;
- prepare requests for the advance of funds; and
- receive such funds on behalf of the UCA.

Note: This is an exception to investigative imprest fund procedures. It allows the contact agent to act as an intermediary between the UCA and the imprest fund cashier.

Each month, the contact agent shall assist the case agent in the preparation of TIGTA Form OI 7520, *Undercover Operations Status Report*.

180.21 Undercover Social Security Numbers.
The NUPM retains records of SSNs assigned to TIGTA. SAC/Directors are responsible for maintaining records of SSNs for each individual UCA assigned to their division. Each SAC/Director may select a Fictitious Identity Package (FIP) Custodian to maintain these records.

180.21.1 Authorization to Use Individual SSNs. Individual SSNs may be used in accordance with the criteria listed in Section 180.22. Only the DIGI may approve using SSNs in Group I UC operations. The DAIGI or respective AIGI may approve using SSNs in Group II UC operations. A separate request is not necessary if the need is stated in the UC proposal memorandum (See Section 180.8.1).

180.21.2 Individual SSNs. Individual SSNs are issued permanently to UCAs s and are used during UC assignments. Individual SSNs may be issued to non-UCAs only if the DIGI, DAIGI, or respective AIGI authorizes them to perform UC duties. At the completion of the assignment, the non-UCA will contact the NUPM for the transfer of the individual SSN.

180.21.3 Transfer of SSNs. SAC/Directors must make written requests through their DAIGI or respective AIGI to the DIGI to permanently transfer SSNs between divisions, to include the return of the SSN to the NUPM.

180.21.4 Social Security Cards Maintenance. The NUPM will send the Social Security card to the UCA upon receipt from the SSA. If the SSN is available before the card is issued, the NUPM may provide the number to the UCA.

Social Security cards will be stored in a locked container maintained by the UCA when not in use. The Social Security card will be utilized by a UCA for undercover operations, in support of a pretext identity or temporarily in connection with activities to update, to enhance the UCA's fictitious identity, or to practice using their fictitious identity. At the conclusion of the activity requiring the use of the Social Security card, it will be returned to a locked container.

180.21.5 Social Security Number Oversight. By February 28th of each year, each SAC/Director will complete annual reviews for the prior calendar year of SSN, tax accounts, credit cards, and banking activity. This responsibility may be delegated to an ASAC/AD or program analyst. Each SAC/Director will include information about FICA/SE postings for the previous calendar year for each SSN in their division in the SAC Certification for Confidential Sources and Fictitious Identities. See Section 180.15.4 and Exhibit (400)-30.2. The certification, with a list of the FIP items for each SSN, will be uploaded to the SAC Certification SharePoint site. A copy must be provided to the NUPM via encrypted e-mail.

The reviews conducted by the SAC/Director will cite adherence to procedures, control weaknesses, and recommend corrective action. Reviews will cover SSN acquisition/disposal, tax return and related document filing, handling of tax refunds and other checks, credit card, and bank account use, etc. As part of the review, the SAC/Director will ensure that there has been no activity on a disposed SSN. A disposed SSN should be examined until the SSN file is destroyed and the number no longer appears on the Master File.

UCAs should contact merchants, banks, and other financial institutions in their respective UC identities to obtain the certification information. Credit reports will only be obtained by the NUPM. During the annual review, the SAC/Director will examine credit reports, bank statements, checkbooks, and other financial records kept by UCAs. SACs will not contact credit bureaus, merchants, banks, or other financial sources. This could compromise UC identities or ongoing operations.

SAC/Directors will obtain transcripts for each SSN by through the Integrated Data Retrieval System (IDRS). The SAC/Director may conduct the inquiry or have an ASAC, SA, or program analyst within the group conduct the inquiry. The UCA to whom the fictitious identity is assigned will not conduct the inquiry. IRS employees shall not be asked to access IDRS in order to obtain these transcripts as this may compromise the UC identities. The SAC/Directors will examine the transcripts or tax data and reconcile any inconsistencies or suspicious activities.

The SAC/Director, or his or her designee, will prepare a memorandum describing the results of the SSN file review. The SAC/Director should secure a copy of the reviewer's memorandum, the formal work papers, and the SAC Certification for Confidential

Sources and Fictitious Identities in a TIGTA safe. Reviews should be conducted and documented by completing TIGTA Form OI 7524, *Fictitious Identity Package Checklist,* and/or TIGTA Form OI 7525, *Individual Social Security Number Control File Checklist,* as appropriate.

180.21.6 Social Security Number Disposal. The SAC/Director must obtain the DIGI's approval to dispose of an SSN. The request for approval memorandum will be sent through the NUPM to the DIGI. Once approved, the NUPM will prepare a memorandum for the SSA documenting the return of the Social Security cards for disposal, and provide the original Social Security cards to the SSA.

180.21.7 Prohibitions and Restrictions. An SSN that has been disposed of may not be used again without permission from SSA and approval by the DIGI.

Agents may not:

- fabricate an SSN for any purpose; or
- use their personal SSN for any investigative purpose.

180.22 Aliases and Fictitious Identification.
UCAs should develop an alias and a permanent FIP, as which will enable them to begin an assignment without undue delay.

180.22.2 Fictitious Identity Package. A FIP consists of personal and financial identification. FIP items essential for an immediate assignment are a fictitious SSN and driver's license. A more comprehensive listing of other important items is contained in Exhibit (400)-180.2. When the DIGI authorizes the transfer of an SSN to another division, the FIP shall also be transferred.

Non-UCA SAs may prepare temporary FIPs if they have written permission from the DAIGI or respective AIGI to participate in a UC operation. These FIPs must be immediately surrendered to the agent's ASAC/AD at the conclusion of the assignment.

180.22.3 Fictitious Identity Package Custody.
The SAC/Director for the field division in which the UCA, or authorized non-UCA SA, is permanently assigned is responsible for controlling that FIP. The SAC may delegate accountability for FIPs to a FIP custodian at the ASAC/AD level.

180.22.3.1 Fictitious Identity Package Custodian Duties. FIP custodian duties for assigned FIPs include:

- annual Inventory of FIP items;
- providing approval for the use of FIP items; and
- maintaining the TIGTA Form OI 7522, *Fictitious Identity Package Usage Log.*

.

FIP custodians must review FIPs, including the discontinued FIPs in their possession, by February 28th of each year. Each FIP custodian submits a memorandum to the SAC/Director detailing the FIP and associated items. The SAC Certification for Confidential Sources and Fictitious Identities will include a list of the FIP SSNs, and will be uploaded to the SAC Certification SharePoint site. A copy of the certification must be provided to the NUPM via encrypted e-mail.

FIP custodians must ensure that all FIP items are provided to the NUPM within 30 days after:

- a SA ceases to be a UCCP member; or
- a non-UCA completes a UC assignment.

180.22.3.2 Fictitious Identity Package Undercover Agent Duties. UCA and authorized non-UCA SAs duties for the FIP include:

- storing FIPs in locked containers when not in use;
- requesting use of FIP items from the FIP custodian via encrypted e-mail; and
- completing the FIP Usage Log when the FIP items are removed for use, and when returned to the locked container.

The NUPM may conduct random reviews of FIP usage, associated documentation, and storage.

180.22.4 Use and Issuance of Fictitious Identity Packages. UCAs or authorized non-UCA SAs may use FIPs only for:

- Performing approved UC assignments;
- One-time assumptions where a pretext identity is required;
- Rehearsing fictitious background and cover stories; or
- enhancing FIPs.

Prior to the deployment of any FIP items, the FIP custodian must approve their use. FIP items may not be used without approval. UCAs, and authorized non-cadre SAs, must send an encrypted e-mail to their FIP custodian requesting the use, and approval must be received prior to engaging in the planned activity. The request will include the following information:

- Case number, if applicable;
- Role description;
- Approval for alcohol consumption, if anticipated;
- Statement of intended use - assignment, practice, or enhancement;
- Date(s) if used for practice;

- Time of day if used for practice;
- Location(s) if used for practice;
- FIP items needed; and
- Expected date of return to the locked container.

The FIP custodian responds with "approved" or "disapproved," and replies to the encrypted e-mail. The FIP custodian also signs and dates the FIP Usage Log, and a copy of the e-mail request is retained with the FIP Usage Log. Undercover operations may involve unanticipated and dangerous undertakings that require quick decision-making, and FIP custodians should consider this when approving items necessary for deployment.

FIP items should not be carried at the same time as true identity documents and law enforcement credentials except where it is mission essential, such as unavoidable transportation considerations, as the fictitious identity could be compromised.

180.22.5 Practice Using FIP. UCAs, and authorized non-UCA SAs, may rehearse UC skills to gain expertise and confidence only after obtaining approval. When rehearsing a fictitious background or practicing their roles for specific assignments, UCAs and authorized non-UCA SAs are considered on official business. They may charge regular and law enforcement availability pay hours for this exercise. This type of activity will never occur on personal time.

Although portraying fictitious roles UCAs, and authorized non-UCA SAs, are on duty as representatives of TIGTA. They are responsible for acting in an appropriate manner and they are subject to the consequences of their actions.

SAs must have prior approval to consume alcohol while on official business. Even with approval, SAs are expected to use moderation and common sense when consuming alcohol. SAs may not participate in unlawful activities while practicing their roles. If, while practicing a UC role, SAs become aware of criminal activity falling under the jurisdiction of another agency, they must follow disclosure guidelines outlined in Chapter 700, Chief Counsel, Section 70.5 of the TIGTA Operations Manual, and report the facts to the proper agency, as appropriate.

UCAs conducting non-case specific UC duties (*e.g.*, backstopping) will annotate their time in CRIMES using Code 94 – UC Cadre Activities (Non – Case).

180.22.6 Compromised Fictitious Identities. UCAs are expected to maintain the confidentiality of their participation in the UCCP, their fictitious identities, and all activities associated with the undercover program (*e.g.*, backstopping, training, techniques, investigations, etc.). UCAs may only disclose this type of information (*i.e.,* identity, participation, and UC activities, *etc.*) as needed for official business purposes (*e.g.,* testifying and/or in connection with prosecution). Any disclosure of such

information for other than official business purposes must be coordinated with the NUPM. Unauthorized disclosure of UC identity, participation, and activities may result in removal from the UCCP.

The deliberate or accidental disclosure of the true identity of a UCA can seriously endanger his or her safety and the security of the entire undercover operation. If the UCA's true identity is disclosed at any time, the SAC/Director will immediately notify the DAIGI, or respective AIGI, and the NUPM, who will determine the appropriate course of action to ensure the safety of the UCA.

If the UCA, ASAC/AD, and/or SAC/Director determines that a fictitious identity is, or may have been compromised, cease using it, including the SSN. The SAC/Director will notify the DAIGI, or respective AIGI, and the NUPM immediately. If all are in concurrence, follow the procedures for "SSN Disposal." The UCA shall cancel and collect all other documents that comprise the UCA FIP and forward these to the NUPM for evaluation or disposal.

The UCA shall request a replacement SSN at the time the compromised SSN is cancelled. A current SSA Form SS-5, *Application for a Social Security Card* must be completed. Contact the NUPM for assistance in preparing the Form SS-5. The UCA shall develop a new FIP once a new SSN is issued.

180.22.7 Fictitious Identity Package Backstopping. Imprest fund requests for regularly purchased FIP items such as post office boxes, cellular telephone minutes or plans, computer data minutes or plans, subscriptions, buyers and automobile club memberships will be directed to the NUPM for approval. The NUPM will provide written approval to the UCA's SAC/Director, who will provide authorization to the divisional imprest fund cashier. The divisional imprest fund cashier will ensure compliance with imprest fund guidelines in Chapter 600, Section 50.9 of the Operations Manual.

180.23 Psychological Support Services Program.
TIGTA contracts with clinical psychologists to obtain professional psychological services for the UC program. Individuals involved in UC operations who wish to speak to or meet with a psychologist relative to that UC operation can telephone the NUPM or contact the contractor directly. Agents may not discuss details of a UC operation with any counselor other than the TIGTA contract psychologist. The IRS Employee Assistance Program counselors will not be used for UC operations purposes. All agents, except for UCCP members, must have DIGI approval before using these psychological services. Because the psychologists are contracted by TIGTA, they do not afford the individual agents absolute confidentiality. Psychologists may share information with TIGTA officials on a need-to-know basis. Contact the NUPM with questions relative to the psychological service contract.

The Psychological Support Services Program provides the following services:

1) Applicants – Requested through the NUPM, psychological services are available to administer a battery of assessment tests and interview UCCP applicants to select the best suited candidates for UC assignments.

2) UC Assignments – Requested through the NUPM, psychological services are available to administer a series of personality assessment tests and to interview a UCA prior to beginning a UC assignment. The psychologist advises the NUPM of the results and helps to identify which agents are best suited for UC assignments.

3) Counseling – Requested through the NUPM, psychological services are available to assist UCAs and IRS employees working covert duties with TIGTA. They offer crisis intervention services and stress management counseling. Psychologists are also available to conduct decompression reviews and counsel UCAs after an assignment terminates.

4) Stress Management – A psychologist can be made available to conduct stress management training during training seminars, UC schools, etc. The NUPM should be contacted for coordination of this training.

DATE: July 1, 2020

CHAPTER 400 – INVESTIGATIONS

(400)-190 Evidence

190.1 Overview.
Evidence collected during the course of an investigation must be properly stored for two important reasons:

- To protect the evidentiary chain of custody; and
- To protect from inadvertent loss, alteration, or destruction.

This Section contains information and procedures for identifying, collecting, documenting, and storing evidence related to an investigation by the Office of Investigations (OI). It is incumbent upon special agents (SA) to be knowledgeable about the instructions and procedures contained in this Section, which include the following:

- Definitions
- Identification and Collection of Evidence
- Handling Bulk Evidence
- Storage of Evidence
- Temporary Release of Evidence
- Forensic Analysis
- Opening and Resealing Evidence Containers
- Packaging and Transmittal of Evidence
- Reviews and Inspections
- Disposal of Evidence
- Abandonment Procedures

The appropriate OI executive may authorize a Special Agent in Charge (SAC) to deviate from the procedures contained in this section on a case-by-case basis. The deviation must be explained in a memorandum and maintained with the Evidence Log, as described in Section 190.5.2.

190.1.1 Acronyms Table.

190.2 Definitions.
"Evidence" shall include any item seized, collected, or surrendered to OI that is deemed to have evidentiary value in a potential criminal, civil, or administrative proceeding in establishing the elements of an offense or the truth of the matter being investigated.

"Chain of custody" refers to the testimonial or documentary link, which establishes the authenticity of an item and is the chronological documentation of the handling of

evidence throughout an investigation. Chain of custody proves that the item offered as evidence in a criminal, civil, or administrative proceeding has a logical connection to the case by establishing that it is the same item taken into custody at the time of its initial discovery.

190.3 Identification and Collection of Evidence.
Generally, the basis for acquiring evidence falls within the following categories:

- There is a reason to believe that the item is evidence of a criminal, civil, or administrative violation;
- There is reason to believe that the failure to take the item into custody for safekeeping will result in the loss, irrevocable damage, alteration, or theft of the item and there is no reasonable alternative that is likely to adequately safeguard the item; or
- The item is contraband.

When collecting evidence, the SA must protect its integrity. This encompasses two equally important concepts: the first is not to add anything to the evidence after it is collected or otherwise alter it, and the second is not to destroy, remove, or contribute to the deterioration of evidence once the item is in the SA's possession.

Whenever possible, the SA must collect the best evidence available, generally the original item. See Federal Rules of Evidence (FRE) for additional information concerning rules of evidence. See Section 200.7 of this chapter for additional information concerning best forensic evidence.

The SA first assuming custody of evidence must:

- Provide a receipt to the individual from whom personal property was obtained, if appropriate;
- Prepare TIGTA Form OI 5397, *Evidence Custody Document (ECD)*;
- Place the evidence in an appropriate evidence container, when feasible, and identify the container with TIGTA Form OI 5396, *Evidence Tag*; and
- Document the receipt of evidence in the Criminal Results Management System (CRIMES). See Section 80.

Receipts will be provided to individuals who provide TIGTA with personal property (*e.g.*, currency, valuables) and expect to have the items returned. SAs will comply with all requirements related to the execution of a search warrant, as provided in Section 140.8. Administratively, a TIGTA Form OI 1932, *Custody Receipt for Personal Property,* or equivalent may be used. When a receipt is provided, it should annotate the condition of the personal property received, including known or visible damage.

Once the evidence retained by OI is properly secured, the SA will enter all available information on the TIGTA Form OI 5397. See Section 190.5.4 for additional information related to evidence custody documents. Complete a TIGTA Form OI 5396, and properly affix it to the evidence. The SA will, if needed, seal the evidence container's unsealed opening or seam with specialized tape designed to indicate tampering and/or unauthorized opening, and sign and date across the tape. A witness is required for the inventory and sealing of evidence containers of:

- Suspected or known illegal drugs;
- Firearms;
- Currency;
- Monetary instruments; and
- High value items.

Specialized instructions may apply for handling certain types of evidence. See Section 190.7 below and Section 200.9 of this chapter for additional information and specialized instructions related to the Forensic and Digital Science Laboratory (FDSL).

If unusual circumstances dictate that the evidence collected should be retained in bulk, SAs must follow the guidance in Section 190.4 related to handling large quantities of evidence.

190.3.1 Specialized Instructions for Certain Evidence. The identification, collection, and storage of certain types of evidence require specialized instructions. Those instructions are set forth below:

190.3.1.1 Documents. Documentary evidence may originate from the subject (*e.g.*, address book), from a neutral third party (*e.g.,* bank records), or from OI activities (*e.g.*, photographs). SAs will obtain the original document or certified copy of official records whenever possible, particularly if it is anticipated the document will be used as evidence in criminal proceedings.

As must be careful not to complete the evidence tag over the top of documentary property creating embedded markings in the documents. Original Internal Revenue Service (IRS) documents of significance, such as tax returns, should be logged into evidence. If requested, a copy of the documents may be provided to the IRS component until such time the original evidence is no longer required by OI. See Section 150.6.1 for additional information related to the control of tax returns and return information.

190.3.1.2 Audio and Video Media. When audio or video media are produced or obtained as evidence, make copies of the original evidence media as soon as practical. If immediate duplication is not possible, place the media in evidence containers and give them to the evidence custodian for proper preservation.

Place the following information on the media, as applicable:

- Case number;
- Subject name or case title;
- Case agent;
- Date, time, and place of recording; and
- Identification as an original or duplicate.

Additional information such as the names of the parties recorded, make/serial number of the recording equipment, and the name of the SA making the recording should be documented on TIGTA Form OI 2028-M, *Memorandum of Interview or Activity*. TIGTA Form OI 5396 will be affixed to the container.

Audio-recorded notes made during the course of, or contemporaneous with, a non-custodial interview are not necessarily treated as evidence and may be treated as investigative notes in accordance with Sections 210.12 and 250.5. The recordings of custodial subject interviews will be treated as evidence in accordance with Section 210.20.

190.3.1.3 Photographs. Photographers are responsible for proper handling and chain of custody of images and evidence photographs until they are transferred to the evidence custodian. Identifying information should be documented on a TIGTA Form OI 2028-M, unless the photographs are obtained from a third party. Such information should include:

- Case number;
- Subject name or case title;
- Name of photographer, if known;
- Date, time and place of photograph, if known;
- Brief description of the photograph;
- Identification as an original or duplicate; and
- Identification of the SA who acquired the photograph, if different from the photographer.

190.3.1.4 Illegal Drugs and Related Hazardous Materials. Suspected or known illegal drugs, to include any containers, packaging, or equipment suspected of containing trace amounts of drugs, must be collected and maintained as evidence.

During a search, the suspected illegal drugs should be photographed, if practical, in their original location prior to removal for processing. Process the photographs as documentary evidence.

The following guidelines apply to the partition of suspected or known illegal drugs into separate evidence items:

- Evidence acquired at different times or locations (*e.g.*, different addresses or different places of concealment at the same address) will be separated;
- Quantities with differing packaging or labeling will be separated; and
- Evidence which appears to be of a different composition (*e.g.*, color, shape of tablets) will be separated unless the several types are commingled to the point of making this impractical.

If the suspected or known illegal drug is loose, badly damaged, or in an untenable container, place it in a substitute container. The substitute container must be uncontaminated and must fully contain and safely preserve the evidence during subsequent handling. When suspected illegal drugs are retained as evidence, the SA and a witness will seal the evidence container, and both will sign and date across the tape.

Exercise care that the evidence does not become contaminated or lost through spillage. If a spillage does occur, submit the evidence recovered from the spillage as a separate evidence item.

Liquids and other items involved in the manufacture of illegal drugs may be hazardous. Contact a representative of the Drug Enforcement Administration (DEA), or a State or local law enforcement agency for assistance prior to handling.

190.3.1.5 Weapons. A weapon is any object that is designed, used, brandished, or intended to be used to inflict bodily harm or property damage. A weapon will be seized as evidence if it was used against an IRS or TIGTA employee while in the performance of his/her duties or against IRS or TIGTA facilities or property. Weapons that are in the immediate reach or control of a subject in a search or arrest situation will be secured , and if the weapon is a firearm, unloaded by an SA or other law enforcement officer familiar with the firearm.

Firearms may be seized if there is reason to believe that:

- The firearm is illegally possessed, illegally obtained, inherently illegal, or was used in a criminal violation;
- A dangerous situation would be created by failing to take the firearm into custody; or
- Failure to seize the firearm for safekeeping could result in the theft or loss of the firearm.

If these criteria do not exist, the firearm should not be seized. If the firearm is not seized, if necessary, the firearm should be unloaded and made safe by the SA most

familiar with it and left at the location where it was discovered in as secure a manner as possible.

If the firearm is to be seized as evidence, the firearm will be unloaded before it is sealed in an evidence container. Ammunition seized will be inventoried and placed into a separate evidence container. When a firearm is retained as evidence, the SA and a witness will seal the evidence container, and both will sign and date across the tape.

As soon as practicable, but no later than 24 hours after an agent has secured the firearm, the agent must query the National Tracing Center by submitting a National Tracing Center Trace Request Form or by contacting the Criminal Intelligence and Counterterrorism Division to submit an “eTrace” request.

190.3.1.6 Currency and Monetary Instruments. Currency and monetary instruments will be counted, and the serial numbers and denominations will be documented on a TIGTA Form OI 2028-M. Alternatively, the currency may be photocopied and the photocopy should be attached to TIGTA Form OI 2028-M. If the currency is photocopied, the copy must be 50% larger or 25% smaller than the actual currency. Photocopying of currency must comply with 18 U.S.C. § 504, to ensure compliance with Federal law. The ”Description of Article” block on the TIGTA Form OI 5397 will include a list containing the serial number and denominations or will reference the attached TIGTA Form OI 2028-M containing the same information.

When currency or monetary instruments are retained as evidence, the SA and a witness will seal the evidence container, and both will sign and date across the tape.

See Section 190.3.3 for special reporting requirements relating to currency and monetary instruments.

190.3.1.7 High Value Items. Jewelry and items of potential high monetary value must be scrupulously accounted for. When high value items are retained as evidence, the SA and a witness will seal the evidence container, and both will sign and date across the tape. Prior to seizing, the jewelry or potential high value item should be photographed. When describing such items, SAs will utilize descriptive wording that does not support a specific value or composition for an item. Wording such as "yellow" in place of specific elemental identifiers, such as "gold" and wording such as "green colored stone" and not "emerald" will be utilized. The SA will include additional photographs of any damage or visible defects, noting the details in the description field of TIGTA Form OI 5397. The evidence custodian should not log or place valuables into storage or remove them from storage without having a witness present. Jewelry and other items having a potentially high monetary value should be kept separate from documentary evidence, whenever possible.

190.3.1.8 Digital Evidence. Digital or electronic evidence may be contained on computers, internal or external storage media, digital cameras, servers, cloud-based platforms, cellular telephones, or on other portable electronic devices. Digital evidence is volatile, fragile, and can be unintentionally altered, damaged or destroyed by improper handling. Whenever possible, SAs who encounter, or believe they will encounter, digital evidence should contact the Digital Forensic Support (DFS) Group for guidance. The Cybercrime Investigations Division (CCID), to include the Cyber Investigative Cadre, should follow CCID divisional guidelines and may contact DFS on an as-needed basis.

190.3.1.9 Material Related to Complaints. Material received related to an intake does not have to be secured in the evidence system; however, the system is available. Items received by TIGTA prior to opening an investigation require reasonable steps to secure them. If transferring material to another OI office, the SA initially receiving the evidence may complete a TIGTA Form OI 5397 to establish the chain of custody. However, a log number should not be assigned at the intake office, but rather at the receiving office that is assigned the case.

190.3.1.10 Extremely Hazardous Materials. An SA shall not take custody of any known extremely hazardous materials including, but not limited to, radioactive, biohazardous, flammable, corrosive, toxic, or explosive materials. Upon encountering such materials, the case agent will contact the appropriate officials (Fire Department, Federal agency, and/or Hazardous Materials Unit), supervisor, and prosecuting officials, as applicable, advising of the material and situation.

190.3.2 Special Agent Responsibilities. All SAs are responsible for the security and chain of custody of evidence in their possession until they release the item(s) to the evidence custodian. The release of evidence from an SA to the evidence custodian must be completed and documented as soon as reasonably feasible, but no more than 10 days after obtaining evidence. In the event that the evidence custodian is unavailable, items of evidence may be deposited into a temporary evidence storage, if available, in accordance with Section 190.5. SAs should annotate the TIGTA Form OI 6501, *Chronological Case Worksheet* (CCW) when evidence is released to temporary storage or the evidence custodian.

SAs will store evidence in their possession in locked containers that only the case SA or other designated SAs can access. SAs may retain working copies of audiotapes, videotapes, and documents with their case files.

190.3.3 Reporting Requirements. Investigative activities that include the identification and collection of evidence items must be documented on TIGTA Form OI 2028-M, which is maintained in the case file, as well as in CRIMES. However, a separate TIGTA Form OI 2028-M documenting the collection of evidence is not required if the collection

of evidence is in conjunction with an investigative activity already documented in a TIGTA Form OI 2028-M (*e.g.*, interview, consent, search of home).

The TIGTA Form OI 2028-M should include the following information:

- A brief description of the evidence, and from whom and when it was obtained;
- If the item collected by TIGTA is a copy, state whether the original is available;
- The identity of the custodian of the original and under what circumstances he/she will release it (*e.g.*, subpoena, court order), if applicable.

The subsequent logging in of evidence does not require a separate TIGTA Form OI 2028-M. Document this information, including the evidence log number, on the TIGTA Form OI 6501.

When special monies or other property of value is collected, including drugs and firearms, there may be additional reporting requirements that are contained in Chapter 600, Section 50.11.8 of the TIGTA Operations Manual. TIGTA Form OI 141, *Statement of Special Moneys and Property Transaction*, shall be completed and submitted as required. Complete Block #11 on TIGTA Form OI 5397 and maintain a copy of the TIGTA Form OI 141 with the TIGTA Form OI 5397.

190.4 Handling Bulk Evidence.
Large quantities of evidence are often collected from a single source during the course of an investigation. As with individual pieces of evidence, care must be taken to ensure the integrity of bulk evidence collected is maintained.

190.4.1 Handling Procedures. Bulk evidence may be collected, retained, and accounted for on a single evidence custody document in lieu of accounting for each item individually on separate forms. Whenever bulk evidence is collected and maintained, the case agent should inventory the items in a timely manner. SAs should consult with the relevant Government attorney to determine if the evidence needs to be sequentially numbered, in the event the evidence is turned over during discovery.

190.4.2 Transfer of Item to Individual Evidence Custody Document. If an individual item included in bulk evidence needs to be transferred or removed, the item should be transferred to an individual evidence custody document. This is accomplished by annotating the “Purpose of Custody Change” block of TIGTA Form OI 5397 related to the bulk evidence with a description of the item(s) and a statement indicating the item will transfer to an individual TIGTA Form OI 5397, including the evidence log number of the new item.

When multiple items of evidence are documented on a single TIGTA Form OI 5397 and part of the evidence needs to be released or transferred, a new TIGTA Form OI 5397 should be completed, which bears the same log number as the original, followed by an

alpha character. The new TIGTA Form OI 5397 lists the item(s) being released in order to maintain the chain of custody for these item(s). The TIGTA Form OI 5397 with the alpha character will remain with the evidence.

190.5 Storage of Evidence.
Each post of duty (POD) where evidence is maintained must have an evidence locker and/or evidence room.

An evidence locker must be:

- A locker or cabinet having an appropriate General Services Administration (GSA) approved lock; and
- Of weight, size, construction, or installation to minimize unauthorized access or theft of evidence.

An evidence room must:

- Have a three-position dial-type combination lock, cipher lock, or similar GSA approved lock, and should be constructed with security and safety in mind. Staff safety, air quality, security, integrity of evidence/property, and the prevention of unauthorized entry should be considered.

The combinations for the evidence locker and/or evidence room should be changed at least every three years, unless conditions dictate sooner. Combinations shall be updated as soon as possible under any of the following conditions:

- When the security equipment is first placed into service;
- When a person knowing the combination no longer requires access to it; or
- When a combination has been subjected to possible compromise, actual compromise, or unauthorized disclosure.

Locations that have the ability to individually assign codes do not need to update combinations when an individual no longer needs access as long as the individual's code is removed. A record that the evidence locker combination has been changed or an individual's code has been deleted will be maintained within the locker.

The evidence custodian may store bulk evidence or oversized items of evidence at an alternate location, provided the alternate location is TIGTA-controlled, secure, and should notify the relevant Government attorney.

All PODs are encouraged to utilize a temporary evidence locker, commonly referred to as a drop-box, if available, when the evidence custodian or alternate is unavailable. A temporary evidence locker should be designed to be accessible to any SA submitting

evidence, but retrieval of evidence can only be accomplished by the evidence custodian or alternate. In circumstances where a temporary evidence locker is not available, the evidence must be secured in a locked container (*e.g.,* desk, filing cabinet) until an evidence custodian is available to secure the evidence into the evidence locker. In the event it is not possible to release evidence to the evidence custodian, the SA will secure the evidence in a drop-box where available. The SA will annotate the Evidence Custody Document and CCW of the case file, deposit the evidence in the drop-box, and will notify the evidence custodian as to the use of the drop-box. Upon return to their duty station, the evidence custodian or his/her alternate will process the evidence.

190.5.1 Evidence Custodian. Assistant Special Agents in Charge (ASACs) are responsible for designating one SA and an alternate SA as the evidence custodians at each POD. Access to the evidence locker or room can only be gained through and in the presence of the evidence custodian or the alternate custodian. The evidence custodian or alternate are the only personnel authorized to have the combination and/or key for such facilities and/or boxes. A historical record of evidence custodians and alternates for each POD will be maintained with the evidence logs.

The custodian or alternate is responsible for:

- Receiving evidence from SAs;
- Placing evidence into evidence storage;
- Removing evidence from evidence storage;
- Maintaining an evidence log; and
- Testifying in court to the evidentiary chain of custody and control of the item.

Evidence custodians will review the evidence tag, evidence custody document, and evidence container with the SA, who will correct and initial all documentation errors when possible. Administratively, the 'Description' of the item annotated on the evidence tag, evidence custody document, and evidence log must be consistent and concise, but need not be verbatim.

190.5.2 Evidence Log. The TIGTA Evidence Log, a standardized bound book, documents and accounts for evidence entry and removal through cross-reference with the evidence custody document and evidence tag. The evidence custodian is responsible for maintaining the log, which must be stored in the evidence locker. The inside cover of the logbook will identify the organization or activity responsible for the evidence room and dates spanned by the entries. Blue or black ink will be used to make the entries.

When logging in evidence, use one page for each evidence custody document referenced regardless of the number of items placed in the evidence locker. Each page will contain the following heading:

- Case title;
- Case number (if applicable);
- Case agent;
- Description of item(s); and
- Date entered into evidence.

Additionally, each page has five columns with the following headings:

- Item number;
- Date;
- Released by;
- Received by; and
- Reason for transfer.

The custodian will annotate the evidence log for the following events, as applicable:

- The initial entry of evidence items into the evidence locker;
- The removal of evidence items from the evidence locker;
- The return of evidence items to the evidence locker;
- The splitting of an evidence item into several items;
- The location of all evidence stored outside the evidence locker, such as items stored in a bank safe deposit box, or as bulk evidence or oversized items stored at an alternate facility; and
- The disposal of evidence items.

Note: The evidence logbook only needs to indicate when an item went in and out and does not need to include every transfer such as to the case SA, to the FDSL, to the U.S. Postal Service, intermediaries, *etc*.

190.5.3 Evidence Tags. A TIGTA Form OI 5396 is completed by the collecting SA and affixed appropriately. The evidence custodian will amend the evidence tag to include the evidence log number in such a way as to minimize possible embedded markings on the evidence.

190.5.4 Evidence Custody Documents. All TIGTA Forms OI 5397 will be maintained by the evidence custodian in the evidence locker as follows:

- Evidence custody documents that pertain to evidence for which the custodian must account will be maintained in numerical sequence in a folder labeled “Active.”
- When evidence is temporarily released from the evidence room, the original evidence custody document will transfer with the evidence, and a copy of the evidence custody document will be retained in the “Active” folder until the

evidence is returned to the evidence room. When evidence is returned, the original evidence custody document will replace the copy in the "Active" folder, and the copy will be destroyed.

- When the approval to dispose of evidence is being obtained, the original evidence custody document will be sent to the final disposal authority, and a copy of the evidence custody document will be retained in the "Active" folder until the original evidence custody document is returned to the evidence custodian.
- When all items of evidence listed on an evidence custody document have been properly disposed of, the original evidence custody document, and any related documents, will be filed in chronological sequence by the date of final disposal in a folder labeled "Inactive." Once the original evidence custody document has been placed in the "Inactive" folder, a duplicate copy should be sent to any TIGTA POD that had previously logged in those items of evidence for their reference, if applicable. Other copies may be destroyed.

A copy of the evidence custody document will be filed in the "Inactive" folder in lieu of the original form, noting the disposition of the original form, if one of the following conditions exists:

- The original evidence custody document is entered as a permanent part in the record of trial;
- The original evidence custody document accompanies evidence permanently released to an external agency;
- The original evidence custody document is filed in the 'Inactive' folder of the TIGTA POD that disposed of the evidence; or
- The document is not available for other reasons.

Evidence custody documents are required to be maintained in the "Inactive" folder for five years following the date of destruction and/or return.

When extra pages are necessary for continuing the chain of custody, the TIGTA Form OI 5397C, *Evidence Custody Document – Continuation Sheet*, will be used. Ensure the log number(s) and page number(s) are entered on the TIGTA Form OI 5397C. The chain of custody will then continue until evidence is disposed of or a new continuation sheet is required.

190.5.5 Grand Jury Materials. SAs who receive material related to grand jury matters (grand jury or Rule 6(e) material) must take special care to prevent its unauthorized disclosure. Grand jury material must be properly secured and identified as grand jury material. Grand jury material may be stored and maintained by the case agent in a locked container or file cabinet. It should be kept separate and not intermingled with other, non-grand jury evidence, but may be kept in the same room or area as other,

non-grand jury evidence. The evidence custodian and alternate should be included on the Rule 6(e) list. See Section 250.25 for additional instructions applicable to Federal grand jury materials.

190.6 Temporary Release of Evidence.
Evidence will be removed from the evidence room only for permanent disposal or temporary release for specific reasons. Examples of temporary release are:

- Creation of working copies;
- Transmittal to the FDSL for forensic examination;
- Transmittal to FDSL for audio/video enhancement; and
- Case presentation at a trial, hearing, and/or mediation.

The person receiving temporary custody of the evidence must safeguard it and maintain the chain of custody until the evidence is returned to the evidence custodian. The evidence custodian will release the original evidence custody document to the person who assumes temporary custody.

Any change in custody of evidence after TIGTA acquires it will be recorded in the "Change of Custody" section of the evidence custody document. If the evidence custodian does not release the evidence to another entity or relinquish control of the item, do not annotate any change of custody, but document the evidence log and ECD remarks accordingly.

When evidence is received from another law enforcement agency, the SA who receives it will inventory the evidence and prepare an evidence custody document. Any receipts or chain of custody documents from the other agency will be attached to the evidence custody document.

When evidence is temporarily released from storage, it shall be returned to storage as soon as practical. The SA will document the CCW of the case file whenever evidence is submitted to, or retrieved from, the evidence custodian.

190.7 Forensic Analysis.
All forensic analysis must be coordinated through the laboratory director or lead examiner, FDSL specialized instructions apply for processing certain types of physical evidence for evaluation by FDSL. In these circumstances, contact FDSL for assistance.

The FDSL operates a Laboratory Information Management System (LIMS) that includes an automated evidence tracking database and barcoding system. The LIMS tracks chain of custody of evidence sent to the FDSL for analysis. The LIMS is authorized for use in place of other requirements in this instruction for the sole purpose of chain of custody while evidence is at the FDSL. LIMS database records will be maintained at the FDSL or in the individual case file if a particular chain of custody is challenged. If

the LIMS is inoperable due to power outage or other technical problem, the FDSL will track evidence via the TIGTA OI Form 5397 and comply with all requirements set forth in this section.

190.7.1 Analysis of Documentary Evidence. Guidance on submission of documentary evidence for forensic analysis is contained in Section 200.

190.7.2 Analysis of Drugs. FDSL does not analyze drug evidence. SAs should notify the laboratory director of the FDSL to employ the services of other laboratory systems. Guidance on the use of other Federal, State or local laboratories is contained in Section 200.

When transferring drugs to a laboratory for analysis, obtain a receipt indicating the:

- Type and amount of suspected drugs by weight or volume;
- Name and address of the laboratory to which drugs are released;
- Name and signature of the person receiving drugs;
- Date of transfer; and
- Name and signature of SA releasing the drugs.

190.7.3 Enhanced Quality Audio/Video Media (Tapes, CD-ROMs, and DVDs). SAs should submit media to the audio/video enhancement specialist at FDSL when the audio or visual quality of the media or portions of the media are poor. FDSL will produce copies with electronically enhanced quality, which will not affect the original media. When submitting audio/video media for enhancement, send the following items:

- Original audio media whenever possible (when it is not possible to send original media, submit high quality copies); and
- Only original video media.

190.7.4 Mailing Evidence for Forensic Analysis. SAs must protect the chain of custody when transferring evidence items through the mail. SAs must employ the services of a reputable courier that provides for the signature release and package tracking. See Section 190.9 for additional information related to packaging and transmittal of evidence. Evidence can also be hand delivered to FDSL or the Technical and Firearms Support Division.

Address evidence to FDSL at:

TIGTA Forensic and Digital Science Laboratory
Attention: Evidence Custodian
12119 Indian Creek Court
Beltsville, MD 20705

190.7.4.1 Requests for Forensic and Digital Science Laboratory Analysis. A request assistance form must be completed via CRIMES prior to obtaining laboratory services.

190.8 Opening and Resealing Evidence Containers.
When opening evidence containers, the SA will physically inventory all items. When opening evidence containers having suspected illegal drugs, firearms, currency, monetary instruments, or high value items, SAs should have a witness present whenever possible.

Evidence containers will be sealed in the manner described in Section 190.3. SAs may utilize the same evidence container and evidence tag previously used if they remain serviceable.

190.9 Packaging and Transmittal of Evidence.
When shipping evidence, all items should be double-packed and labeled with the complete mailing address and complete return address on both the inner and outer shipping containers. When packaging evidence for transfer, the evidence container with evidence tag affixed, along with the original evidence custody document, will be securely sealed within the external mailing container. Also include an emergency contact number. The word "evidence" shall not appear on the outer wrapping.

Prior to shipping any electronic or digital evidence, an SA should consult with FDSL for specific instructions and to ensure the selected delivery method does not employ any methods that could damage the evidence. Additionally, when shipping digital evidence, proper care should be taken to protect the items from electrostatic shock through the use of electrostatic bags. Protect all digital evidence, regardless of media type, from physical alteration, damage, and vibration/shock by using the proper packing materials when placing items inside the inner shipping container.

The employee initiating the shipping process is responsible for:

- Contacting the employee on the receiving end of the transfer and identifying an appropriate means for transporting the item that is cost effective while maintaining adequate security;
- Notifying the employee on the receiving end when the item was shipped, the estimated arrival date, a description of the items being shipped, and the package tracking number assigned by the shipping service;
- Following up to ensure that the package has arrived at its final destination;
- Contacting the shipping service, if utilized, to immediately initiate procedures to track and locate the missing package should the package not arrive within the expected delivery period; and
- Addressing all evidence that is being shipped to the FDSL to the attention of the evidence custodian.

In circumstances which require the shipment of original evidence that, if lost, could not be duplicated or reproduced, and if hand delivery by the agent is not possible, coordinate the shipping of those items with the UPS Express Critical - Secured Product Division at 1-800-714-8779 inside the U.S. and Canada or 1-913-693-6205 outside the U.S. and Canada. The use of this service will result in significant increased shipping cost and must be approved by the SAC responsible for paying the charge.

190.10 Reviews and Inspections.
SACs, ASACs, and the Operations Division's Inspection Team have the authority to inspect or review any and all items associated with evidence. During these administrative reviews, the reviewers may ask evidence custodians to open evidence containers to verify an item or count money. Evidence custodians must remain with the reviewers while they are conducting their reviews. Custodians will annotate the evidence custody document to indicate the opening and resealing of evidence containers. Because custodians never relinquish control of the property, reviewers are not part of the chain of custody.

190.10.1 Evidence Storage Inventory Audits. A full physical inventory shall be conducted by the primary and the alternate evidence custodian each calendar year and whenever there is a non-temporary change in the incumbent in that position. An evidence custodian will provide the ASAC with a memorandum that states the results of the audit and any discrepancies that were identified by the audit, with a copy stored in the evidence room. Prior to the change in incumbent, the incoming and outgoing evidence custodian should jointly conduct the physical inventory audit. A separate audit by the evidence custodian does not need to be done in a calendar year in which an inspection is taking place that includes an evidence review.

190.11 Disposal of Evidence.
The case agent must obtain approval from the ASAC for the final disposition of evidence. To ensure a proper custody chain, evidence must be returned to the case agent prior to its destruction and/or return. With the written approval of the ASAC, as indicated on the evidence custody document, the case agent initiates the disposal of evidence when:

- Cases are closed without prosecutions or referrals for administrative adjudication. For referrals of TIGTA documents or other evidence (*e.g.,* photographs, video files, etc.) to another agency for possible prosecution or administrative action, retain the item(s) and contact the TIGTA Disclosure Officer prior to making any referral. See Chapter 700, Section 70.5 and Chapter 700, Section 50 of the TIGTA Operations Manual regarding disclosure and referral procedures.

- For cases that have been prosecuted or administratively adjudicated and after the defendant/subject has exhausted all appeals, the case agent should obtain concurrence for disposal from the Government attorney.
- As determined by the ASAC, further retention of the evidence is no longer required.

TIGTA Form OI 5397 allows for split disposal of items when applicable. Obtain ASAC approval in Block #13 *Final Disposal Authority* of the evidence custody document for disposal of items specified. If additional approval is required for disposal of other items at a later date, obtain ASAC approval for additional items in the second portion of Block #13. Additional disposal approvals and actions can be recorded in Block #15. The evidence custodian records the final disposition date in the evidence log and on the TIGTA Form OI 5397, Block #14. Once all items listed on the custody document have been disposed, the TIGTA Form OI 5397 is maintained in chronological sequence in the "Inactive" folder within the evidence locker.

See Chapter 600, Section 50.11 of the TIGTA Operations Manual for procedures relating to accounting for seized assets, bribes, and restitutions as they relate to Form OI 141.

190.11.1 Disposal of Small Quantities of Drugs. Evidence custodians shall dispose of small quantities of drugs in a manner that completely destroys them. Various local environmental and safety laws may apply, creating a complicated regulatory environment for what destruction methods are allowed. If an SA is unsure of the best way to destroy small quantities of drugs in their jurisdiction, the SA should contact their local law enforcement partners for assistance. A second SA or law enforcement officer should witness the destruction.

190.11.2 Disposal of Large Quantities of Drugs. Large quantities of drugs, defined as amounts commensurate with manufacture or distribution, will be transferred to local, State, or Federal law enforcement agencies with appropriate training and facilities to safely dispose of the drugs.

The ASAC's authorization is required for an SA to transfer drugs to another law enforcement agency for destruction. In this situation, SAs must obtain a receipt from the agency representative indicating the:

- Type and amount of drugs by weight or volume;
- Name and address of law enforcement agency to which drugs are released;
- Name and signature of person receiving drugs;
- Date of transfer; and
- Names and signatures of SAs releasing drugs.

The transfer will be annotated in Block #14 of TIGTA Form OI 5397 and in the evidence log.

190.11.3 Disposal of Firearms. Return a seized firearm to its rightful owner or designee unless it has been forfeited to the Government or is contraband. Within 10 days following a determination that a firearm can be disposed of, the case SA will attempt to locate the rightful owner. A firearm will be returned to the rightful owner, under controlled circumstances, if the firearm can be legally possessed by the owner and such return would not place the owner in violation of Federal, State, or local law. See 18 U.S.C. § 922(g) for categories of persons prohibited from receiving, possessing, or affecting commerce of a firearm.

If the case SA is unable to locate the owner or the owner is unknown, then the case SA must initiate abandonment proceedings. See Section 190.12 for abandonment procedures.

The transfer of all firearms returned to their rightful owners will be annotated in Block #14 of TIGTA Form OI 5397 and in the evidence log.

If a firearm was seized as evidence, and the owner of the firearm is convicted of an offense involving the use of the firearm, the Assistant United States Attorney should be asked to request that the court include an order summarily forfeiting the firearm to the United States pursuant to 18 U.S.C. § 924(d)(1) as part of the Judgment and Commitment Order. Firearms that fall within this category will be retained until all judicial proceedings have been completed then transferred to the National Firearms Agent Safety and Tactics (FAST) Coordinator for disposal.

Firearms that become the property of the Government may be added to the OI firearms inventory or disposed of in accordance with 41 CFR Parts 102-40 and 102-41 (See §§ 102-40.175 and 201-41.190-200).

The National FAST Coordinator will dispose of all firearms. When a firearm is to be disposed of, the Divisional FAST Coordinator (DFC) will contact the NFC for disposal instructions. See Section 130.19.

190.11.4 Disposal of Other Personal Property. Disposition of personal property is defined in 41 CFR § 102-41. Return personal property that was obtained/seized to its rightful owner unless it has been forfeited to the Government, kept by request of the court or Government attorney, or is contraband. Within 10 days following a determination that personal property, other than a firearm, can be disposed of, the case SA will attempt to return the property to its rightful owner.

If the case SA is unable to locate the owner or the owner is unknown, then the case SA must initiate abandonment proceedings. See Section 190.12 for abandonment procedures.

Return original IRS documents to the function from which they were obtained, and file original affidavits in the TIGTA case file.

The transfer of all personal property returned to its rightful owner will be annotated in Block #14 of TIGTA Form OI 5397 and in the evidence log.

Original recordings of court ordered nonconsensual intercepts, transcripts of such recordings, and dialed number recorder (DNR) data obtained in connection with such intercepts must be retained as evidence for a period of 10 years from the date the recording was made, as required by 18 U.S.C. § 2518. At the end of this retention period, the recordings may only be disposed of pursuant to a court order.

190.11.5 Disposal of Electronic Media. If returning electronic media, and such media contains contraband (*e.g.* personally identifiable information which is not the owners, credit card information track dumps, child pornography), TIGTA personnel will delete all contents contained thereon to ensure no contraband is returned.

190.12 Abandonment Procedures.
Voluntary abandonment must be pursuant to 41 CFR § 102-41.85. Where property cannot be returned, the case SA, with the approval of the SAC will initiate abandonment proceedings as follows:

- If the owner of the property is known, the SAC will notify the owner by certified mail at the owner's last known address of record that the property may be claimed by the owner or his or her designee and, that if the property is not claimed within 30 days from the date the letter of notification is postmarked, title to the property will vest in the United States. See Exhibit(400)-190.1 for the letter format;
- If the owner of the property is unknown and the estimated value of the property less than $500, the SAC will post notice. The notice must be published once a week for at least three successive weeks and contain the information as referenced in 41 C.F.R. § 102-36.330. The property must be held for a period of 30 days from the date of the first publication of notice. Upon expiration of the 30 days, title vests in the United States; and
- If the owner of the property is unknown and the estimated value of the property is less than $500, no notice is required and the property will be held for 30 days. Upon expiration of the 30 days, title vests in the United States.

Pursuant to 41 C.F.R. § 102-41.130, there is a three-year period in which the claimant can file a claim for the abandoned property. All abandoned property where title vests in

the United States will be maintained in the evidence locker for a period of three years from the date of vesting of title in the United States. If the abandoned property in question cannot be secured in the evidence locker, the property will be stored securely in a cabinet, locker, or room that is located within a secure TIGTA-controlled area which minimizes the possibility of unauthorized access, loss, or theft. If upon expiration of the three year period, title to the property still vests in the United States, the property will be disposed of in accordance with 41 C.F.R. Part 102-41.

DATE: April 1, 2020

CHAPTER 400 – INVESTIGATIONS

(400)-200 Forensic and Digital Science Laboratory

200.1 Overview. The Forensic and Digital Science Laboratory (FDSL) is the scientific investigative arm of TIGTA. Its primary responsibility is the forensic evaluation of physical and digital evidence encountered by Special Agents (SAs) during investigations. Another major role is the formulation of sound scientific policies and procedures as they relate to forensic aspects of physical and digital evidence (*e.g.*, handling, collection, chain of custody, *etc.*) and analysis using valid protocols.

This section contains information related to the following:

200.1.1 Acronyms Table.

200.2 FDSL Technical Staff.
In addition to conducting scientific examinations of physical and digital evidence, the FDSL's technical staff:

- Offers expert advice and assistance in processing crime scenes, to include documenting and collecting physical evidence;
- Provides expert testimony before judges, juries and other adjudicative bodies;
- Advises and assists the U.S. Attorney's Office (USAO) in the evidentiary significance and presentation of expert testimony; and

- Instructs others in the basic and advanced investigative aspects of the forensic sciences.

Staff examiners maintain close liaisons with other Department and TIGTA components, Federal law enforcement laboratories, and professional forensic organizations to:

- Stay abreast of the latest advances in equipment, techniques, and methods adopted for the evaluation of physical and digital evidence; and
- Identify sources to help SAs with the examination of physical evidence beyond current FDSL capabilities (*e.g.*, deoxyribonucleic acid (DNA) testing, explosives, arson, firearms, trace evidence, and narcotics.)

200.2.1 FDSL Evidence Custodians. The FDSL has an evidence custodian and alternate(s) who are responsible for:

- Receiving evidence;
- Placing evidence into evidence storage;
- Removing evidence from evidence storage;
- Maintaining the chain of custody in the Laboratory Information Management System (LIMS); and
- Testifying in court to the evidentiary chain of custody and control of the item.

A historical record of evidence custodians and alternates are kept by the quality assurance manager.

200.2.2 Specialty Areas and Typical Analyses Performed. Typical analyses performed by the FDSL are briefly described in the chart below.

Specialty Area	Typical Analyses Performed
Questioned Documents	• Evaluate handwriting, signatures, and hand printing to establish authorship of questioned writing. • Detect and decipher alterations, erasures and obliteration of entries. • Compare, classify and identify sources of printed matter (*e.g.*, typewriters, laser, dot matrix, ink-jet printers). • Establish a link or common source between questioned and known materials (*e.g.*, photocopies, writing inks, papers, printers, typewriters, torn documents). • Conduct or arrange for physical or chemical analysis of inks and paper. • Reconstruct or piece together cut, torn, or shredded documents. • Preserve and enhance burnt or water-soaked documents.

	• Determination of genuine vs. counterfeit documents. • Evaluate items for investigative lead information, *e.g.*, anonymous note investigations for indented writing impressions. • Decipher original text from single-strike, carbon film printer ribbons. • Determine toner code sources through U.S. Secret Service laboratory.
Digital Forensics	• Forensic imaging, analysis, and reporting of digital evidence examinations. • Preparation of search warrants and subpoenas. • Production of electronic evidence, equipment, and related media. • On-site participation during execution of search warrants. • Participation in subject, witness, and third-party interviews. • Testimony concerning the content of digital evidence at judicial and administrative proceedings. • Open-source and Internet-related research to support TIGTA investigations. • Consultation with SAs concerning all aspects of digital evidence. • Providing technical training to SAs, upon request.
Latent Prints	• Process and examine evidence for latent prints. • Compare patent/latent prints with known exemplars. • Compare unknown to known impressions to confirm identity. • Enter and search unidentified latent prints in the Next Generation Identification System (NGIS). • Download criminal fingerprint records for comparison purposes. • Obtain civil fingerprint records from the Federal Bureau of Investigation (FBI).
Digital Image Processing Non-Video Formats	• Process photographic images and damaged documents for purposes of improving the visual appearance and readability of the evidence. • Image processing as a secondary technique to improve the visibility of details in developed fingerprints, alterations, erasures and obliterated entries.
Graphics Preparation	• Create courtroom demonstration charts, photographs, and enlargements. • Create training or presentation materials. • Create publications including newsletters, brochures, and posters.

General Crime Scene Processing	• Respond to scenes and assist in searching, processing, and collecting evidence. • Conduct searches and evaluate scenes for physical evidence. • Photograph crime scenes. • Collect and properly package physical evidence.
High-Resolution Digital Photography	• Capture images of physical evidence. • Record results of laboratory examinations.
Audio/Video Enhancement	• Multimedia file format conversion. • Redaction of audio and/or video events. • Video clarification examinations. • Maintain the integrity of original images. • Image processing clarification examinations. • Storage of image files to include data integrity and compression. • Audio clarification examinations.

200.3 External Agency Assistance.
Resources allowing, the FDSL will assist other law enforcement organizations with forensic examinations and seizure of digital evidence. Any forensic examination conducted for an external organization will comply with the FDSL policies and procedures and the TIGTA Operations Manual. Requests for FDSL assistance must be on agency letterhead and submitted to the Assistant Inspector General for Investigations-Cyber, Operations, and Investigative Support Directorate.

200.4 Forensic Quality Management System.
The FDSL maintains accreditation with the American National Standards Institute American Society for Quality National Accreditation Board (ANAB). This accreditation requires the implementation of an extensive quality system that ensures the integrity of the system.

The FDSL has instituted many policies and procedures that are in compliance with ANAB AR 3125 *Supplemental Requirements for the Accreditation of Forensic Science Testing Laboratories* and ISO/IEC 17025:2017, *General requirements for the Competence of Testing and Calibration Laboratories.* The policies and procedures that ensure compliance can be found in the FDSL's Quality Assurance Manual (QAM).

Because of the FDSL's unique role within OI and the FDSL adherence to ANAB accreditation requirements, the FDSL has instituted some policies and procedure involving the evidence handling process that differ from other sections of this manual. The policies and procedures are outlined in detail within the QAM and the Evidence Handling SOP.

200.5 Laboratory Information Management System.
The FDSL maintains the LIMS, which is a system that houses the chain of custody of items within the FDSL's custody, and used to assign and track the case work, and is used to produce FDSL reports. The LIMS is a key component of the quality system. The LIMS is used in place of TIGTA Form OI 5397, *Evidence Custody Document*, while items are within the FDSL's custody. LIMS tracks items electronically and all FDSL personnel have unique bar codes that are scanned when evidence changes custody. The secured digital signature replaces inked signatures found on the Evidence Custody Document.

200.5.1 Secondary Evidence. Secondary evidence is evidence generated by examiners in the course of their examinations such as developed fingerprints and electrostatic detection apparatus (EDSA) lifts. Secondary evidence is entered into LIMS and stored in the FDSL evidence room for safekeeping.

200.6 Advantages of Early FDSL Involvement.
Early FDSL involvement will ensure:

- The best forensic evidence is collected and submitted for evaluation;
- Forensically significant evidence is identified;
- Suitability of evidence for scientific evaluation is determined;
- Crime scenes are processed using proven techniques for collecting, packaging and preserving fragile evidence from further deterioration;
- New techniques or methods are not employed for the evaluation of physical evidence until adequately tested and verified by scientific methods;
- Evidence is developed to its fullest evidentiary potential;
- Investigative resources are redirected when evidence clearly refutes an allegation or witness statement;
- SAs are referred to accredited laboratories for evidence testing beyond current FDSL capabilities;
- The law enforcement community is educated on the significance of forensic examinations, current capabilities and procedures for the collection of appropriate exemplar materials;
- A proper legal basis exists for any subsequent seizure;
- The proper seizure, packaging and storage of electronic media; and
- The proper documentation of original evidence to be submitted to the DFS program for storage and processing.

200.7 Best Forensic Evidence Rule.
SAs consider physical evidence within a legal context. The FDSL evaluates the same evidence within a scientific context to establish its forensic significance.

When latent print processing is performed prior to evaluating items for trace materials, significant evidence is destroyed and/or lost. Trace evidence (*e.g.*, indented handwriting impressions, hairs, fibers, *etc.*) often offers circumstantial leads which may prove beneficial in identifying a suspect. Forensic laboratories follow a strict analysis sequence for the examination of physical evidence to preserve all trace evidence for subsequent laboratory testing.

SAs must submit original evidence when available. Do not submit copies and retain originals in evidence vaults. An examination of copies may result in less than definite conclusions.

When a photocopy, microfilm, or fax copy constitutes “original” evidence, submit it as an original and identify it as the best available "copy." Do not photocopy evidence copies and submit these. SAs should locate and submit the earliest generation copy for analysis. Evidence that is repeatedly photocopied loses details and/or introduces defects. Both situations hinder laboratory examinations and contribute to less than conclusive opinions.
Laboratory opinions are dependent upon the quality and/or quantity of evidence, questioned and known, submitted for evaluation.

200.8 Request for Laboratory Services.
SAs should provide laboratory examiners with sufficient case background for the examiner to understand the evidence within the context of the investigation.

The FDSL maintains field requests for laboratory services in a database. To properly associate supplemental requests with previously evaluated evidence, the FDSL retains related case evidence under one common laboratory identifier. Therefore, it is important for SAs to refer to this unique identifier when they submit supplemental evidence referring to the same investigation and/or field case identifier.

To request services from the FDSL, a Request Assistance Form (RAF) must be submitted in CRIMES. In instances where a RAF is unable to be submitted (*e.g.,* an Intake), complete Form OI 7535, *Request for Forensic Laboratory Services*, and e-mail the request to *TIGTA Inv Forensic Science Lab Requests. Analysts cannot begin working on a request until a written request has been received.

200.8.1 Requests for Expedited Laboratory Services. If the seriousness of the allegation or the type of evidence demands expeditious handling, the SA should notify the FDSL Laboratory Director and their immediate supervisor as soon as possible. If made on behalf of an Assistant United States Attorney (AUSA), the SA may send a formal written request detailing the specific reasons for requesting expedited analysis.

When time constraints imposed by circumstances of the investigation and/or by a trial date impact the professional duty of its examiners, the FDSL Laboratory Director

reserves the right to refuse to evaluate evidence. Final decisions regarding acceptance and expeditious handling are within the purview of the FDSL Laboratory Director.

To request a change in case priority for an analysis that has already been submitted, the SA must contact the Laboratory Director, through their supervisor, as soon as possible.

200.8.2 Request to Out-Source Laboratory Examinations. If SAs encounter physical evidence that cannot be examined by the FDSL (*e.g.*, DNA, arson, explosives, hazardous materials, firearms, tool marks), they should contact the FDSL for information on forwarding their evidence to reputable forensic laboratories for evaluation or send the evidence to the FDSL so that the laboratory may facilitate the transfer of evidence for them. SAs are requested to notify the FDSL laboratory director before submitting evidence to another laboratory.

200.9 Laboratory Evidence Submission Policy.
Evidence submitted to the FDSL is accepted with the understanding that it has not been, nor will it be, examined for the same purpose by another laboratory system on behalf of TIGTA. This is considered opinion shopping and will not be supported by the FDSL. The FDSL reserves the right to refuse to examine evidence that has been evaluated by another laboratory for the same purpose except under compelling circumstances. The FDSL may also refuse to examine evidence for any reason that compromises the quality of an examination, the exercise of professional duty, or the safety of laboratory personnel or facilities.

If evidence submitted consists of grand jury materials covered by grand jury secrecy rules, notate the request. This ensures the FDSL implements appropriate procedures. SAs should place the names of all laboratory personnel on the grand jury list. Due to assigned duties for evidence processing, technical reviews, *etc.*, all personnel will have access to the evidence and information while in the laboratory's custody.

Any physical evidence that could potentially be contaminated by unknown biological, chemical or other hazardous materials will not be forwarded to the FDSL. See Section 120 for information on responding to critical incidents. Once the substance is identified as non-hazardous, the SA may forward the evidence to the FDSL for forensic testing. A copy of the testing lab's report must accompany the Request for Laboratory Services.

The use of other Federal, State, or local laboratories is *only* authorized under the following circumstances:

- If another laboratory previously examined evidence in the investigation and a supplemental examination becomes necessary, then submit this supplemental request to this same laboratory; or

- If in joint agency investigations in which TIGTA is not the lead, the lead representative wants to engage the services of another laboratory; or
- If the FDSL is unable to accommodate the time constraints imposed by circumstances of the investigation or required capabilities; or
- If the forensic request falls outside of current FDSL capabilities (*e.g.*, DNA, firearms, explosives).

The FDSL is not equipped (*e.g.,* specialized mechanical hood systems, storage or instrumentation) to analyze unknown liquid/powder substances for biological or chemical source determinations. Other qualified laboratories must conduct these analyses prior to submitting physical evidence to the FDSL for subsequent testing. Contaminated evidence that has not been properly tested will be returned to the SA unexamined.

200.9.1 Submission of Physical Evidence. All physical evidence that requires a forensic analysis must be hand-delivered or submitted via overnight courier to the FDSL. See the FDSL Intranet homepage for the physical and mailing address. SAs must employ the services of reputable courier that provides for signature release and package tracking (*e.g.*, United Parcel Service). Without such services, it is difficult to establish a chain of custody. The use of First Class mail is not an acceptable means to submit evidence to the laboratory unless there is a tracking number associated with the submitted items. Evidence can also be hand-delivered to the FDSL. Address evidence to the FDSL Custodian.

200.9.2 Submitting Digital Evidence for DFS Examination. After a DFS examiner has been assigned, the case agent should arrange directly with DFS the transfer of any evidence required for the analysis or forensic duplication. Digital evidence is fragile and can be unintentionally altered, damaged, or destroyed by improper handling and storage. Items submitted for examination should be packaged to minimize the possibility of damage and shipped using an authorized overnight courier, *e.g.*, UPS or FedEx. Each package should contain Form OI 5397, *Evidence Custody Document*. See Section 190.

If the forensic examination is to include media that is not from the Internal Revenue Service (IRS), the case agent must provide the DFS examiner with documents that establish the legal authority for the examination such as a search warrant, subpoena, court order, or consent.

200.9.3 Submission of Supplemental Evidence. When supplemental evidence is located for analysis after the FDSL has issued its findings, the SA shall follow all instructions outlined in this section as they pertain to original case submissions. The SA shall use the previously assigned laboratory unique identifier. Some cases do not require resubmission of original evidence.

200.9.4 Evidence Receipt Letter. Upon receipt of physical evidence, the FDSL generates an Evidence Receipt Letter and forwards it to the SA and the approving official by e-mail. This letter outlines the following case-specific information for SAs:

- Date and how the evidence was received;
- The field case number and title;
- The assigned laboratory unique identifier and submission number; and
- The assigned laboratory section including the section lead examiner's contact information.

If SAs have questions regarding their case submissions, they should refer to this correspondence and consult the section lead examiner.

200.10 Return of Evidence.
Upon completion of requested examinations, the FDSL will return all evidence to the case agent along with laboratory reports. Items will be sealed in evidence envelopes with evidence tape. All evidence will be returned using an overnight courier or the case agent will be notified to pick up his/her evidence.

200.11 Protecting the Integrity of Physical Evidence.
SAs must protect physical evidence within the legal context of their investigations as soon as possible and adopt procedures that protect it within its forensic context accordingly. Evidence should be treated as if a forensic laboratory will conduct an examination at a future date during the investigation. Protecting the integrity of physical evidence encompasses two equally important concepts:

- Do not add anything to evidence after it is recovered; and,
- Do not destroy, remove, or contribute to the deterioration of potential evidence once it is in the investigator's possession.

Collect and package known and questioned items separately. The SA must protect evidence against cross-contamination.

SAs must conscientiously evaluate the potential value of physical evidence, including documents, and protect it accordingly by adopting the following practices:

- Wear gloves when handling evidence;
- Make copies of evidential documents and use these for review rather than handling original evidence;
- Do not write on top of evidence, to include writing on Post-It Notes, or complete evidence envelope entries after enclosing evidence items, as writing on top of original evidence adds indented writing impressions that can obscure crucial evidence;

- Do not fold, staple, or otherwise mutilate evidence;
- Do not circle areas of interest on original evidence;
- Protect paper documents in document protectors;
- Protect magazine stock paper in paper folders;
- Protect non-porous items of evidence in boxes, envelopes or paper bags;
- Always store evidence at standard temperature and humidity (office environment); and
- Always store original evidence away from direct sunlight and at ambient room conditions. Sunlight fades documents and high heat and humidity can damage documents, inks, and fingerprint evidence.

200.11.1 Coated Paper and Non-Porous Items. Evidence such as coated, shiny paper (***e.g.***, magazine paper) and non-porous items such as glass, metal, or plastic must not be preserved in plastic. Plastic creates static that contributes to the deterioration of latent/patent prints. These items should be packaged in paper.

200.11.2 Photocopies and Laser Printed Items. Evidence that consists of photocopies or laser printed material should be placed in archival quality document protectors. Copier and printer toners stick to non-polypropylene plastics which can damage the "original" evidence item. If archival quality document protectors are not available, use heavy stock paper folders instead.

200.11.3 Thermal Facsimile Items. Evidence such as original thermal facsimile copies should be immediately photocopied to preserve the text on the document and readability. Older technology thermal facsimiles may deteriorate over time, especially when exposed to extremes in temperature and humidity to the point where the original text is no longer visible.

200.11.4 Biological Evidence. Biological evidence (***e.g.***, blood, semen, saliva, DNA, urine, hair, skin cells) is susceptible to contamination and degradation unless it is properly preserved and stored. Heat and moisture contribute to the bacterial degradation and contamination of suspected biological stains and can destroy their evidentiary value. Contact the FDSL for advice regarding the examination of physical evidence for serological and/or DNA characterization. State/local accredited forensic laboratories may accept Federal evidence for analysis. If necessary, contact an accredited commercial laboratory that will analyze samples for a fee. Contact the FDSL for assistance in locating a testing facility.

Laboratories, including the FBI, will not conduct examinations of unknown stains for DNA typing without known comparison/elimination samples from both the victim, suspect, and the SAs in contact with the item.

200.11.5 Unknown Substances. SAs should obtain thorough testing of an unknown substance to identify the source of the substance (*e.g.*, liquid, powder, etc.) The FBI system will provide a formal test report. Formal test results should be accompanied by a formal report identifying the unknown material. Only then can personnel be assured that no health or hazard exists. A copy of this report must be forwarded to the FDSL along with evidence request for more traditional examinations.

200.11.6 Marking Physical Evidence. Do not mark evidence prior to submitting for laboratory testing. If evidence must be marked, place initials, date, or other identifying marks in an inconspicuous location on the item. For documentary type evidence, the reverse lower right hand corner is a suitable location. Known documentary evidence should be initialed and dated on the back of the document by the SA as obtained. Use indelible inks such as ballpoint pens or fine-tip markers in blue or black. Do not use unusual colors (*e.g.*, pink, red, green) or markers that can bleed-through paper. If an item is not amenable to ballpoint pens or fine-tip markers, use a fine-tipped permanent marker; place a small label on the item and enter identifying information; or place the item in a suitable container and mark the container.

Unless necessary, do not use exhibit numbers. The FDSL uses a standard numbering system that ensures consistency in reporting and allows for the addition of supplemental exhibit numbers as necessary. The court will assign its own exhibit numbers.

200.12 Packaging Physical Evidence for Submission.
Cross-contamination destroys forensic and evidentiary value therefore it is important to prevent the cross-contamination of evidence. Carefully preserve questioned and known evidence separately. When properly packaged, lab examiners can eliminate the possibility that other evidence sources, either questioned or known, have contaminated the questioned evidence item(s).

When packaging items for submission to the FDSL, follow procedures which protect the evidence's integrity and that clearly identify the articles for technical examiners. When appropriate, place evidence in evidence envelopes and seal using tamper-proof evidence tape. Items too large for envelopes should be packaged in suitably sized containers and sealed using evidence tape.

Establishing a legal chain of custody is paramount if evidence is to be presented and accepted at criminal prosecution. Include Form OI 5397, *Evidence Custody Document*, with the submission.

If SAs encounter unusual classes of evidence, contact FDSL personnel for guidance and specific instructions for packaging and protecting the items during transit.

200.12.1 Sharp Objects. Sharp objects (*e.g.*, syringes, razor blades, *etc.*) that require forensic examination must be handled appropriately as they pose potential health and physical hazards. Sharp objects must be packaged in containers to prevent them from potentially cutting or nicking examiners. Laboratory requests must indicate the presence of sharp objects to adequately alert examiners to the hazard.

200.12.2 Potentially Hazardous Materials. When packages contain potentially hazardous materials, indicate this on all packages to alert FDSL examiners to the potential hazard. Unknown spills or biological/chemical materials must be collected and evaluated by trained specialists, at the scene.

200.12.3 Evidence for Latent Print Examination. When submitting evidence for a latent print examination, use packaging procedures designed for the evidence type.

200.12.4 Paper Evidence. Paper evidence (*e.g.*, documents, forms, currency) must be sealed in archival quality plastic document protectors (polypropylene). For a slick paper surface, such as magazine stock, SAs must package these items in heavy stock paper folders.

200.12.5 Non-Porous Evidence. If evidence consists of a non-porous surface (*e.g.*, plastics, wallets, computers, firearms, metals, razors), protect the item in a suitably sized cardboard box and stabilize it for transit with pieces of rolled paper.

200.12.6 Indented Writing Impressions. Evidence suspected of having indented writing impressions should be packaged between sheets of thin cardboard.

200.12.7 Shredded Documents. Shredded documents should be collected in their original container without disturbing the layers. The container should then be packaged in a box that prevents movement during transit. Confining the contents prevents the disturbance of layers and makes reconstruction somewhat easier.

200.13 Questioned Documents.
The forensic specialty of questioned documents covers a broad spectrum of case types, handles a wide variety of evidence types, and answers varied investigative questions. Questioned document examiners examine evidence items that depict written or printed communications such as checks, tax returns, corporate contracts, facsimiles, or printouts, but that may also include items such as writing in lipstick on a mirror, a cut-and-paste threat, a suicide note, shredded documents, or burned or faded documents. Some of the typical investigative problems answered by a forensic document examiner include:

- Identification or elimination of the suspected author of questioned writing (signatures, initials, numerals, extended letters, forms, etc.);
- Identification of forgeries or non-authentic signatures;

- Identification of a common source between materials (photocopier trash marks, typewriter font damage, torn edges);
- Typewriter comparison or identification;
- Identification of the authenticity of material (*e.g.*, genuine or counterfeit documents);
- Deciphering original text (erasures, overwritten, obliterated entries, printer ribbons);
- Printer ribbons for case-sensitive text;
- Establishing the method of production;
- Lead information – indented impressions, identify equipment used such as typewriter, printer, photocopier, writing instrument, and;
- Determination of common authorship of writings, even if no suspect(s) have been determined yet.

Typically, document examinations are dependent upon a side-by-side comparison of questioned and known items. SAs bear the responsibility for collecting not only questioned evidence but also known exemplar materials. Known exemplar materials can consist of handwriting, copies made on suspected photocopiers, samples of typewriting taken from suspected machines, samples of check stock from victim, printer ribbons, *etc.*

200.13.1 Known Exemplar Writing. Known exemplar writing consists of genuine specimens that represent the natural handwriting and full range of variation of the person's writing. These specimens serve as the sole basis for comparison with questioned writings.

Exemplar writing falls into two categories:

- Collected course of business writing, and
- Dictated writing.

Collected exemplars are genuine writings prepared in the normal course of social, occupational, or business activities. Dictated writing, whether provided voluntarily or pursuant to grand jury subpoena, are writings prepared by an individual on demand by the SA for the sole purpose of comparison with questioned writing. See Exhibit(400)-200.1.

For handwriting comparisons, known exemplars must meet the following criteria:

- Exemplars must be in the same style as the questioned writing (*i.e.*, printed or cursive);
- If the questioned writing consists of signatures and/or initials, the known exemplars must consist of the same name or initials; and

- The known exemplars must contain the same text, words, letters, numbers and combinations as the questioned writing.

200.13.2 Authentication of Known Evidence. SAs should contact FDSL document examiners for guidance, recommendations, and assistance prior to obtaining directed, request exemplar writing.

200.13.3 Legal Requirements of Authentication. When obtaining/collecting known handwriting evidence, SAs must keep in mind the legal requirements of authentication. Federal Rule of Evidence (FRE) 901(a) requires that the proponent of evidence must present proof that the item is what the proponent claims it is. The evidence must be sufficiently proven as being from a particular person before the trial judge will allow their admission into evidence. FRE 901(b) outlines the procedure for determining authenticity. The showing of authentication represents a special aspect of relevancy, a dependency upon a condition of fact. Title 28 U.S.C. § 1731 also governs the admissibility of handwriting for purposes of comparison. Where an SA personally obtains evidence directly from a particular individual, the SA's testimony as a witness with knowledge will satisfy FRE 901(a). See FRE (b)(1).

If the SA collects other writings, such as those written in the course of a person's everyday activities, authenticity must be established circumstantially. The legal test is whether there is sufficient evidence to support a rational finding that the collected writing is that of a particular person. Thus, the collection of such writings must be carefully considered. It is the SA's responsibility to obtain the foundational information and/or testimony necessary for proof of authorship. There are a number of well-settled approaches to circumstantially establishing authenticity. See FRE 901(b) (2), (4), (7) and (10), and Title 28 U.S.C. § 1731 (including interpretive notes and decisions). Many times an official of the agency which obtained and stored the records may testify to their authenticity, even if the writing was not witnessed by that official.

The forensic document examiner cannot authenticate the known writing samples. Also, if a laboratory opinion is based upon the compilation of known writing submitted and some samples are not admitted, the document examiner must conduct another examination to determine whether the remaining evidence is sufficient to support the opinion expressed.

If the writer is present pursuant to a grand jury subpoena, he/she is directed to provide normal and natural handwriting samples in the type and amount determined by the SA. If the individual attempts to thwart efforts to obtain normal and natural samples of his/her writing, explain that he/she can be held in contempt of the grand jury subpoena.

200.13.4 Obtaining Request Exemplars. SAs should contact a questioned document examiner to discuss the suitability of evidence for a forensic examination and for specific guidance prior to gathering exemplar materials for comparison.

When obtaining request exemplars, review each item as it is removed from the writer. Ensure the writing resembles samples of his/her normal course-of-business writing. If the writing appears slow and labored or rapid and scrawled, the writer may be attempting to disguise his/her writing. To break conscious attempts at disguised writing:

- Show the writer known samples of his/her course of business writing. Ask the writer to remove his/her license, other forms of identification, *etc.* and to compare these with the writing provided. Request the writer use his/her normal and natural handwriting to complete the exemplar materials;
- Request the writer change his/her slant of writing;
- If the writer states that he/she has multiple styles of writing, gather samples of each different style;
- Ask the writer to prepare several samples using his/her unaccustomed hand;
- Dictate totally unrelated material;
- Take a break and distract the writer from the act of writing; and,
- Speed up the dictation.

200.13.5 Mechanics of Obtaining Dictated Handwriting Samples. To obtain dictated handwriting samples:

- SAs should approach the session as a specialized type of interview.
- The subject writer should be comfortably seated at a table and provided with a writing instrument.
- The subject writer should be given only one exemplar form at a time to complete.
- All material should be dictated to the writer as to writing style and text (*e.g.*, "Print the following return address on the envelope: John P. Smith, 123...").
- Upon completion, the exemplar form should be removed from the writer's view.
- Another blank exemplar form is then given the writer, and the process repeated.
- Each page should be sequentially numbered by the SA as they are collected from the writer. This process is continued until the desired number of samples is obtained for each questioned writing.
- A black ink ballpoint pen should be used for writing at least half of the samples. If another type of writing instrument was used to produce the questioned material, then a similar writing instrument can be used for some of the samples.
- When dictating, the questioned material must be read verbatim to the writer without suggestion as to the arrangement of material, capitalization, and/or punctuation.

SAs should not assist the writer with spelling or other format directions; however, the examiner may need examples of the exact same letter combinations so, in some of the later exemplars, the SA should dictate spelling if required. The pace of dictation should

be such that the subject writes continuously while completing each exemplar form. The SA should vary the pace of the dictation with some of the subsequent repetitions.

In general, the SA should:

- Continue the dictation regardless of thwarting efforts because the more writing obtained, the better it is for the examination; and
- Attempt to recreate the environment when the questioned documents were drafted as much as possible.

200.13.6 Handwriting Opinions. Occasionally, physical evidence may be of limited value or unsuitable for a document examination. The FDSL will evaluate each item or case on its own merits and make that determination on a case-by-case basis.

Handwriting opinions are expressed in terms of a subjective probability (*i.e.*, it cannot be equated to a numerical probability). Examiners of the FDSL use the professional terminology expressed in the Scientific Working Group for Forensic Document Examiners, "Standard Terminology for Expressing Conclusions of Forensic Document Examiners." This standard explains the 9-point conclusions used. SAs are referred to this document for clarification.

The nine-point opinions used by examiners of the FDSL include:

- Identification/Elimination: identifies or eliminates a known writer as the author of the questioned writing;
- Highly Probable Did/Did Not: there is a high degree of agreement/non-agreement between the known and questioned writing; however, some major writing feature that is present is not reflected in the known/questioned writing;
- Probably Did/Did Not: there is a high degree of agreement/non-agreement between the known and questioned writing; however, several significant features are not reflected in the known/questioned writing;
- Indications Did/Did Not: there is agreement/non-agreement between the few significant features reflected in the known/questioned writing; however, the evidence is far from conclusive. This opinion often is used to develop investigative leads; and
- No Conclusion: there is insufficient evidence to point towards or away from a writer.

200.14 Latent Prints.
The specialty of latent prints covers:

- The visual examination of physical evidence for the presence and collection of patent prints;

- Physical and/or chemical processing of evidence to develop latent (invisible) prints (for the purpose of this section the term “latent print” will be used when referring to an unknown print whether it be patent or latent);
- The comparison of 10-print cards to confirm identity;
- The comparison of known prints to latent prints for identification; and
- NGIS entry and search of unidentified latent fingerprints.

Successful latent print evaluations are dependent upon the development of quality latent prints and being in possession of quality known prints. Known prints are categorized as victim/legitimate elimination prints or suspect prints. The examination of overlapping prints can be a challenge, but does not necessarily destroy the opportunity to identify a suspect’s prints. Additionally, depending on the type of surface; as long as evidence is properly stored and protected, latent prints can remain for years. However, the longer latent prints remain unprocessed on porous surfaces, the more difficult they become to visualize using traditional processing methods.

200.14.1 Suspect/Victim Inked Prints. Excessive case turnaround times in the latent section are a direct consequence of examiners having to re-evaluate unidentified latent prints. To reduce turnaround times, SAs should submit known prints for comparison (suspect) and elimination (legitimate) purposes. Although the FDSL understands that occasionally the SA has developed no suspect, individuals with legitimate access to the evidence can provide elimination prints.

By eliminating legitimate prints during the evaluation phase, examiners can concentrate their efforts on the identification of suspect prints. Many prints developed by the FDSL include not only fingers, but also palms. If possible, SAs should also collect palm impressions along with standard 10-print inked fingerprint cards.

200.14.2 Requests for Civilian/Criminal 10-Print Cards from the FBI. When requesting the comparison of a specific person, insure all pertinent information is provided in the request (*e.g.*, subject’s full name including aliases, married name, and maiden name; Social Security Number; race; sex; date of birth; FBI number, if known, and if the subject is a Government employee) to the FDSL. If the FBI is unable to locate a requested card, the FDSL will notify the SA as soon as possible.

Local law enforcement agencies are an excellent source for 10-print cards. Some local agencies also fingerprint subjects arrested for certain misdemeanors and they often obtain palm prints. Advise the local agency that the print cards being requested are for latent comparison purposes. This ensures the FDSL obtains a good quality copy.

200.14.3 Next Generation Identification System. NGIS is a storage, search, and retrieval system for digitized fingerprint images. There are national, State, local, and regional NGIS databases. The system searches its database and provides a "candidate list" of the closest matching fingerprint images. A fingerprint specialist examines the

results and determines whether further examination is necessary. FBI 10-print files of Government employees/applicants, armed forces, and civilian positions requiring background fingerprinting, and palm print files are not automated. The system now also includes palm prints.

200.14.4 Latent Opinions. Within the forensic latent print discipline, examiners may reach one of three conclusions; identification, exclusion or inconclusive. The TIGTA Latent Print Section defines these as:

Identification:
"Source" identification is an examiner's conclusion that two friction ridge skin impressions originated from the same source. This conclusion is an examiner's decision that the observed friction ridge skin features are in sufficient correspondence such that the examiner would not expect to see the same arrangement of features repeated in an impression that came from a different source and there are insufficient friction ridge skin features in disagreement for an examiner to conclude that the impressions came from different sources.

The basis for a "source" identification conclusion is an examiner's decision that the observed corresponding friction ridge skin features provide extremely strong support for the proposition that the two impressions came from the same source and extremely weak support for the proposition that the two impressions came from different sources. A "source identification" is a statement of an examiner's belief (an inductive inference) that the probability that the two impressions were made by different sources is so small that it is negligible. A source identification is not based upon a statistically-derived or verified measurement or comparison of all friction ridge skin impression features in the world's population.

Exclusion:
"Source" exclusion is an examiner's conclusion that two friction ridge skin impressions did not originate from the same source. The basis for a 'source' exclusion is an examiner's decision that there are sufficient friction ridge skin features in disagreement to conclude that the two impressions came from different sources.

Inconclusive:
Inconclusive is an examiner's conclusion that there is insufficient quantity and clarity of corresponding friction ridge skin features between two impressions such that the examiner is unable to identify or exclude the two impressions as originating from the same source. The basis for an inconclusive conclusion is an examiner's decision that a source identification or source exclusion cannot be made due to insufficient information in either of the two impressions examined.

An inconclusive conclusion is reached due to a number of reasons; they include but are not limited to: overall poor quality of known exemplars; the area of friction skin needed

for comparison was not recorded on the known exemplar; the quantity and/or quality of friction ridge detail is limited in the latent print; fully recorded tips, sides, joints, and palms are necessary.

200.15 Digital Forensics.
The specialty of digital forensics includes:

- Forensic imaging, analysis, and reporting of digital evidence examinations;
- Preparation of search warrants and subpoenas;
- Production of electronic evidence, equipment, and related media;
- On-site participation during execution of search warrants and seizures;
- Participation in subject, witness, and third-party interviews;
- Testimony concerning the content of digital evidence at judicial and administrative proceedings;
- Open-source and Internet-related research to support TIGTA investigations;
- Consultation with SAs concerning all aspects of digital evidence; and
- Providing technical training to SAs, upon request.

See the DFS Forensic Guide for more information on DFS program procedures.

200.15.1 DFS Examiners. DFS examiners are responsible for performing timely analysis of electronic evidence submitted to their laboratory. Within five days of the receipt of evidence, the assigned examiner will contact the case agent to have a comprehensive discussion concerning the overall investigation and the role of the digital evidence examination. Recognizing that each digital evidence examination is unique, the following are some possible discussion topics:

- Range of examination capabilities;
- Establishment of examination purpose, scope, and specific goals;
- Development of keyword search list;
- Known skill-set of computer user, including countermeasures, encryption, and passwords;
- Overall priority of the examination, including investigative or judicial deadlines;
- Grand jury information; and
- Review of search warrant, when appropriate.

200.15.2 DFS Support. Once the request for DFS assistance has been assigned, the DFS examiner is available to assist with the following aspects of the investigation:

- Development of the investigative plan by providing input that may impact legal issues, decisions to seize or copy evidence, and the acquisition of additional support, equipment and supplies; and

- Coordination of equipment and resources needed to conduct a search warrant. The equipment and resources needed will be based on the following:

    - Number and types of computers involved;
    - Location of computers within the overall search site;
    - Type, topology, and operating system of any computer network involved;
    - Size and nature of data storage media and the existence of any "back-up" media;
    - Level of cooperation expected from the computer owner and their degree of sophistication;
    - Remote connectivity issues;
    - Type of software involved;
    - Nature of any computer security, passwords or encryption utilized; and
    - Discussion of the computer aspects of the search warrant with the advising AUSA.

See the guidance documents in the DFS Library for additional information on searching and seizing computers.

200.15.3 Documenting the Examination Results. At the conclusion of the examination, the DFS examiner will discuss the findings with the case agent and determine if there are any additional leads or evidence items to review. The DFS examiner will prepare and submit a Form OI 7580, *DFS Forensic Examination Report*, of the findings to the DFS Assistant Special Agent in Charge (ASAC) for review and approval. The approved Form OI 7580 will be provided to and discussed with the case agent. See the DFS Forensic Guide, Sections 3, 6, and 7, for more information on pre- and post- digital forensic examination procedures and required documentation.

200.15.4 Storage of Digital Evidence. Digital evidence in the possession of the DFS Group will be stored in accordance with the policy and procedures in Section 190. Given the nature of electronic evidence, circumstances may dictate that digital copies be maintained in mass electronic storage requiring specialized evidence handling and documentation.

There may be cases where a digital forensic copy or image is generated by DFS and the original evidence, such as a physical laptop computer or cellular telephone is returned to its owner. In such instances, the digital copy produced by DFS will be considered “best evidence” and the case agent will coordinate with the DFS examiner to ensure the Form OI 5397, *Evidence Custody Document*, is prepared and maintained by the appropriate field division.

200.15.5 Computer-Related Investigations. SAs should be familiar with conducting computer-related investigations and should note the following when investigating a computer incident:

- The success of any data recovery/analysis and resulting potential prosecution is dependent on the actions of the individual who initially discovers a computer incident;
- Whenever possible, isolate the suspect computer from additional use or possible tampering. The entire workspace is a potential crime scene, not just the computer itself;
- Preserve evidence in its original state. Opening a file on a computer system changes it. Once the file is changed, it is not original evidence and may be inadmissible in any subsequent proceedings. Opening a file also alters the computer generated time and date showing when the file was last accessed/created and could make it more difficult to determine who committed the violation or when it occurred;
- Computer disks, CD-ROMs, tape storage media, and additional hard drives found in the area of the suspect computer need to be protected and isolated. Prevent unauthorized individuals from access to the device(s) involved;
- The initial responder may be called to testify concerning measures that were taken during the initial computer system shutdown or isolation. The SA should take detailed notes, photographs, sketches, and video recordings during the scene processing. This will also help ensure the appropriate evidentiary chain of custody;
- The initial responder to a computer incident should secure the scene and immediately contact a DFS examiner for further guidance and assistance; and
- Initial interviews of potential witnesses and/or suspects may be enhanced by consultation with a DFS examiner.

If a TIGTA office becomes aware of electronic harassment or Internet-related threats directed at the IRS or an IRS employee, DFS assistance should be requested as soon as possible. Once notified, the DFS ASAC will assign a DFS examiner as a technical advisor to assist during the investigation.

See the guidance documents in the DFS Library for additional information on computer investigations and electronic evidence.

200.16 Multimedia Section.
The Multimedia Section offers a wide range of assistance to TIGTA agents to include:

- Preparation of photographic arrays and graphic displays;
- Digital photography;
- Digital image processing; and
- Audio/video enhancement;

- Other services.

200.16.1 Photographic Arrays and Graphic Displays. The FDSL can assist SAs with photographic arrays. Since photographic arrays must be consistent in both photograph size and format, black and white, the FDSL has several options available to meet these legal requirements.

The FDSL can provide the following types of graphic displays for courtroom demonstrations, presentations, *etc.*:

- Hand-held 8”x10” court charts;
- Handwriting comparison charts;
- Fingerprint comparison charts;
- Poster-sized charts;
- Bound booklets and pamphlets; and
- Slideshow presentations.

200.16.2 Digital Photography. By request, the FDSL captures record-copy images of incoming evidence. Once the evidence is examined and analyzed, photographs may be taken of the processed evidence to document the results. The FDSL offers the following digital photography services:

- Photography of evidence;
- Photo enlargements from photographs or negatives; and
- Photo printing from digital image files or video stills.

200.16.3 Digital Image Processing. Digital image processing is used to resolve case problems involving poor image quality, background interference, or images and text that are not legible. Digital image processing improves the visibility of details such as:

- Image brightness and contrast;
- The readability of indented impressions or damaged documents; and
- Image details in photographs, obliterations, erasures, and image quality.

200.16. 4 Audio/Video Enhancement. Audio and video enhancement may include:

- Multimedia file format conversion;
- Redaction of audio and/or video events;
- Video clarification examination;
- Maintain the integrity of original images;
- Image processing clarification examination;
- Storage of image files to include data integrity and compression; and
- Audio clarification examination.

200.17 Other Services.
The FDSL can provide other services in a limited capacity, to include general training and crime scene processing.

200.17.1 General Training. The FDSL will provide training to internal and external stakeholders on an as needed basis. For field agents, the FDSL training will include instruction for the proper handling of evidence and provide a general overview of forensic services that are provided by the laboratory. The FDSL also provides training for career examiners working for our counterparts at other government agencies. This training can be used for continuing education purposes and/or career development.

200.17.2 Crime Scene Processing. The FDSL can assist agents with searching, processing and collecting evidence from a location or respond to process items that cannot be sent to the lab. The benefits of laboratory assistance include:

- Properly documenting the scene and identifying any potential hazards (chemical, biological or physical) that may be present;
- Properly locating, processing, collecting, and packaging evidence;
- Assist with identifying other forensically significant evidence;
- Photographic recording of a scene; and
- Allowing the SA to focus on other aspects of the case.

200.18 Reports of Examination.
The FDSL issues official laboratory reports of examination for each analysis conducted. These reports follow a uniform format and include the following sections:

Section	Description
Evidence	The dates and how the FDSL received the exhibits. Each questioned and known exhibit will be designated with an exhibit number and a brief description of the item.
Purpose of Examination	Brief statement of why the questioned exhibits were examined (*e.g.*, to establish the author of the written material, to decipher erased entries).
Results and Conclusions	A statement as to the results of examination in the form of an expert opinion.
Disposition of Evidence	Where the evidence will be sent following the completion of that particular examination.
Remarks	If the opinion is less than conclusive, the examiner will suggest ways to remedy shortcomings (*e.g.*, submission of additional known writing that repeats the text of the questioned material).

The technical examiner issues and signs the laboratory report. Reports are returned to the SA by overnight courier and/or e-mail.

200.19 Expert Testimony.
When expert testimony is anticipated, contact the technical examiner immediately. Provide the examiner with an anticipated date for testimony along with the name and contact number for the AUSA. It is imperative for technical examiners to meet and discuss their testimony with the AUSA. This pre-trial conference ensures the AUSA understands the significance of the expert opinion as well as any potential problems that may be encountered with less than conclusive opinions. SAs should ask the AUSA to forward a subpoena to the examiner. This is particularly important when an expert is on call for multiple trials.

200.19.1 Supplemental Materials. On occasion, the FDSL may be asked to furnish supplemental materials (*e.g.*, Summary of Expert Testimony) when requested by defense counsel, or supporting information for Daubert/Frye suppression hearings. Contact FDSL examiners as soon as possible to give them sufficient time to prepare these materials. Summaries of testimony include examiner qualifications, an explanation of the analyses requested, the evidence evaluated, the techniques used, the basis/theory of the techniques employed, the conclusions reached, and any limitations of the methods. Summaries of Expert Testimony replace the examiner's testimony. Judges review them and ultimately determine whether or not the examiner will be permitted to testify at trial as an expert witness.

200.19.2 Courtroom Demonstration Materials. Examiners will discuss the use of courtroom demonstration materials with the SA and/or AUSA. If it is agreed such materials would be helpful, the SA may be requested to return all original evidence to the FDSL for creating these materials.

DATE: July 1, 2017

CHAPTER 400 – INVESTIGATIONS

(400)-210 Interviews

210.1 Overview.
This section contains the following information regarding investigative interviews conducted by TIGTA-Office of Investigations (OI):

210.1.1 Acronyms Table.

210.2 Privacy Act of 1974.
The Privacy Act of 1974 provides safeguards against an invasion of privacy through the misuse of records by Federal agencies, and imposes certain restrictions on the Government concerning collection of information about individuals.

210.2.1 Requirements under the Privacy Act. The Privacy Act requires that each agency maintaining a system of records (*i.e.*, where information is retrievable by name of an individual or by some other personal identifier) must inform each individual whom it asks to supply information of the following:

- Authority for solicitation of the information;
- Whether disclosure of such information is voluntary or mandatory;
- Principal purpose for which the information is intended;
- Routine uses which may be made of the information; and
- Effects on the individual, if any, of not providing all or any part of the information.

This information may be provided to the individual on the form the agency uses to collect the information (*i.e.*, Privacy Act Notices), or on a separate form that can be retained by the individual.

See TIGTA's System of Records Notice, 81 FR 78298 for the routine uses of the information maintained in its system of records.

210.2.2 Collection of Information from the Subject Individual. Under the Privacy Act, special agents (SAs) are obligated to collect information "to the greatest extent practicable" directly from the subject individual. Whether or not it is "practicable" to interview the subject first necessarily depends upon the circumstances of each case.

The Office of Management and Budget Privacy Act Implementation Guidelines and Responsibilities suggest several factors be evaluated in making a determination on "practicability." These factors include:

- The nature of the program (*i.e.,* where the kind of information needed can only be obtained from third parties, such as investigations of possible criminal misconduct);
- The cost of collecting the information from the subject as compared to the cost of collecting it from a third party;
- The risk that the information to be collected from the third party, if inaccurate, could result in an adverse determination;
- The need to ensure the accuracy of information supplied by an individual by verifying it with a third party; and
- Once the agency has determined that it was not practicable to obtain the information from the subject, the provisions for verifying the third-party information with the subject whenever possible.

Courts have approved other considerations as well. For example, it would be appropriate for an SA to contact third-party witnesses prior to contacting the subject of the investigation where the subject is in a position to intimidate third-party witnesses or alter evidence.

When seeking objective, unalterable information, the SA should consider interviewing the subject first, particularly if the subject's ability to coerce a third-party witness or alter evidence is practically nonexistent.

TIGTA procedures regarding the collection of information in non-criminal investigations have been disseminated to bargaining unit employees and are available on the Internet at www.treas.gov/tigta/oi_interview.shtml, paragraph 17.

210.2.3 Documentation of Upfront Subject Interview Decision. In each case, briefly document on the Form OI 6501, Chronological Case Worksheet (CCW), why a subject was or was not interviewed at the beginning of an investigation.

210.2.4 Privacy Act Notices. The Privacy Act requires that notification be given to individuals from whom TIGTA is collecting information in specific situations. At the beginning of an interview of an individual who is the subject or third-party witness in an administrative (non-criminal or non-prosecution) complaint or investigation, furnish the individual with one of the following Privacy Act notices and explain the notice to him/her.

210.2.4.1 Privacy Act Notice 416 (Tax Practitioner Interview). This notice must be provided to all enrolled tax practitioners and unenrolled tax preparers who are the subject or third-party witness of an administrative (non-criminal or non-prosecution) complaint or investigation.

210.2.4.2 Privacy Act Notice 417 (Employee Interview). This notice must be provided to all employees who are the subject or third-party witness of an administrative (non-criminal or non-prosecution) complaint or investigation.

210.2.4.3 Privacy Act Notice 425 (Non-Employee Interview). This notice should be provided to all non-employees who are the subject of an administrative (non-criminal or non-prosecution) investigation, other than enrolled tax practitioners and unenrolled tax preparers (see Privacy Act Notice 416 above). There may be circumstances where the issuance of this notice may not be feasible (*e.g.,* volatile situations). SAs should exercise good judgement and consult with their Assistant Special Agent in Charge (ASAC) for additional guidance. If issuing forms is not feasible, document the reason on the OI Form 6501.

This notice must be provided to all non-employees who are third-party witnesses in an administrative (non-criminal or non-prosecution) complaint or investigation, other than enrolled tax practitioners and unenrolled tax preparers (see Privacy Act Notice 416 above).

Note: The Privacy Act does not require notices be given when interviewing subjects of investigations for ministerial purposes, such as correction of financial statements or related employment application forms.

See Exhibit (400)-210.2 for use of appropriate forms during TIGTA interviews.

210.2.5 Pledges of Confidentiality to Third-Party Sources of Information. Under the Privacy Act, the identity of persons furnishing information in administrative (non-criminal or non-prosecution) complaints and investigations will be protected only when those persons have been given an expressed pledge of confidentiality. Confidentiality under the Privacy Act may not be assumed, and must be invoked by the third-party witness. Do not actively offer confidentiality to a third party or ask the witness to request confidentiality.

Note: Privacy Act confidentiality is not the same as the presumption of confidentiality for Treasury employee complainants under the Inspector General (IG) Act, which must be offered and specifically waived by the employee complainant. See Section 210.4 for information regarding Treasury employee confidentiality under the IG Act.

When interviewing third-party witnesses in administrative (non-criminal or non-prosecution) complaints or investigations, notify the witness:

- Of the applicable Privacy Act authority and routine uses (*i.e.,* how the information is going to be used) by providing the relevant Privacy Act Notice, depending on whether the individual is an employee, tax practitioner, or non-employee. See Section 210.2.4 and Exhibit (400)-210.2 for use of appropriate forms during TIGTA interviews; and
- After giving the above notice, if the third-party witness requests confidentiality, consider granting confidentiality where there is a compelling reason to do so.

Document compliance with the Privacy Act requirement by annotating the issuance of the relevant Privacy Act Notice (*e.g.,* Privacy Act Notice 416, 417, 425), in the opening portion of Form OI 2028-M, Memorandum of Interview or Activity.

If a third-party witness requests and is granted confidentiality under the Privacy Act, treat the witness as a one-time source (See Section 150.3.1) and document that confidentiality was granted on the Form OI 2028-M. If the third-party witness requests confidentiality under the Privacy Act, but the request is denied for lack of a compelling reason, document the request, denial, and general reason for the denial of confidentiality on the Form OI 6501.

A promise of confidentiality is presumed not to exist in any instance where a witness furnishes an affidavit.

210.3 Interviewing Complainants.
The interview of a complainant is often the investigator's first chance to gather information concerning an allegation. Therefore, the complainant interview must be as thorough and detailed as possible. Every effort should be made to conduct the interview in person within 15 days of receipt of the complaint.

210.3.1 Conducting the Complainant Interview. When interviewing complainants, be considerate, understanding, tactful, and impartial, regardless of the motive for the complaint. Inform complainants that the information will be evaluated promptly.

210.3.2 Advising Complainants of Investigative Status or Results. If the complainant asks to be advised of the status and/or results of an investigation, **do not provide the case number or confirm the existence of an investigation. Only the TIGTA Reference Number should be disclosed when speaking to a complainant.** See the Disclosure to Complainants (Victims and Witnesses) card for additional information. Advise the complainant that he/she may file a Privacy Act and/or Freedom of Information Act (FOIA) request with the TIGTA Office of Chief Counsel, Disclosure Branch. Information on filing a FOIA request can be found on the public website (www.treasury.gov/tigta) in the "FOIA" tab or under the "For Citizens" section. See Chapter 700, Section 60 for additional information regarding FOIA requests.

210.4 Confidentiality of Employee Complainants.
All Internal Revenue Service (IRS), Treasury, and TIGTA employee complainants are presumed to have confidentiality under Section 7(b) of the IG Act, unless they specifically consent to allow TIGTA to disclose their identities. The Inspector General, or designee, has the authority to disclose the identity of the employee if it becomes unavoidable during the investigation. Certain disclosures, such as disclosures to Department of Justice (DOJ) officials, or disclosures to management when necessary for administrative action, are considered unavoidable.

The right of confidentiality should be explained to the employee; however, it should never be expressed or implied that the individual's identity will never be revealed. Efforts should always be made to independently verify information provided by any individual to avoid jeopardizing the confidentiality of the individual. Circumstances where it may be necessary to disclose the employee's identity should be discussed with the employee during the interview.

If it becomes necessary to release the name of an employee complainant who has expressed a desire to maintain confidentiality, the circumstances of the release and the person authorizing the release should be documented on Form OI 6501. The circumstances should include the reason, the individuals who are receiving the information, and the date of the release. The case agent should contact the employee complainant prior to the release to advise him/her of the decision to release his/her identity.

Employee complainants who express a desire to maintain confidentiality are considered one-time sources. See Section 150.3.1. If an employee waives confidentiality by consenting to disclosure of his or her identity, such consent should be documented on Form OI 2028-M.

If an employee will be providing continuing information or services to TIGTA, consider designating the employee as a confidential source. See Section 150.3.

Except for limited grants of third-party witness confidentiality under the Privacy Act as described in Section 210.2.5 above, employee witnesses should not be designated as one-time sources regarding information they submit in response to questions concerning an official inquiry. Always include the identity of the employee witness in Form OI 2028-M unless a pledge of confidentiality has specifically been requested and granted. See Section 210.2.5. If information provided by a witness is relevant to an eventual adjudication of the case, the Form OI 2028-M will be included as an exhibit to the Report of Investigation (ROI). If the information provided by the witness is not relevant to the investigation, the Form OI 2028-M should not be included in the ROI.

If an employee witness initiates a complaint regarding a different matter, the employee is assumed to have confidentiality regarding that information, and will be considered a one-time source relative to that information if confidentiality is not waived. This portion of the interview should be treated as a separate interview for reporting purposes, including documentation of whether the individual (now the complainant) waived confidentiality.

210.4.1 Delegation of Authority. TIGTA Delegation Order No. 26 documents the levels of TIGTA management who are delegated the authority to disclose the employee's identity when unavoidable during the course of an investigation. For all investigative matters, this authority is delegated to the Special Agent in Charge (SAC) or higher. Disclosures to DOJ are further delegated to an ASAC or higher.

210.5 Interviewing Employees.
The decision to interview or not interview an IRS employee who is the subject of an employee investigation should be made on a case by case basis and consistent with the Privacy Act. SAs should make every effort to conduct an in person interview of an IRS employee who is the subject or witness in an employee investigation.

If an extenuating circumstance exists, such as a cost prohibitive geographical situation, after consultation with your ASAC, SAs may consider conducting a telephonic interview of the IRS employee, as appropriate.

For interviews regarding criminal violations, the appropriate DOJ or other prosecuting official should be consulted about interviewing the subject employee. See Section 210.13.

When interviewing employees, different guidelines apply based upon whether the employee is a bargaining unit or non-bargaining unit. An employee's employment and bargaining unit status may be determined by contacting the IRS, reviewing the IRS

Discovery Directory, and/or checking the Treasury Integrated Management Information System (TIMIS).

210.5.1 Employee Defined. Persons are considered employees as long as they are listed in the current employment records of any IRS personnel function, including the Office of IRS Chief Counsel, regardless of leave status. The employment status may be:

- Permanent Full-time
- Interim
- Temporary
- Part-time
- Seasonal
- When Actually Employed

Employees in non-work status (*e.g.,* seasonal employees, furloughed employees), absent without leave, or serving disciplinary suspensions retain their employment status.

Contract and lockbox employees are not considered IRS employees for the purposes of this section.

210.5.2. Bargaining Unit Employees. Employees are considered to be members of a bargaining unit if their position is represented by the National Treasury Employees Union (NTEU). Currently, NTEU represents all professional and non-professional employees of the IRS, excluding all employees of the Chief, Criminal Investigation; some employees of the Office of Chief Counsel; employees of the Office of International Operations assigned to overseas posts-of-duty; temporary employees with no reasonable expectancy of continued employment; management officials and supervisors; guards other than protective officers at the Enterprise Computing Center – Martinsburg, West Virginia; and employees described in 5 U.S.C. § 7112 (b)(2), (3), (4), (6), and (7).

A bargaining unit employee:

- May request representation by NTEU in interviews;
- May or may not be a dues-paying member of NTEU; or
- May be temporarily assigned to perform duties of a non-bargaining unit position, but is still considered a bargaining unit employee (*e.g.,* acting manager, etc.).

210.5.3 Non-Bargaining Unit Employees. Non-bargaining unit employees may be NTEU dues-paying members, but have no statutory right to, and are not entitled to, NTEU representation in interviews.

210.6 Conducting the Interview.
The attitude and demeanor of the investigator contributes immeasurably to the success of an interview. The investigator must not exercise authority in any manner that unnecessarily embarrasses or degrades the person being interviewed. Whenever practical, two TIGTA SAs should participate in interviews.

It is important to obtain useful information from the interview and to have good documentation of the information provided in the interview. Look at interviewees when asking them questions and during their responses to evaluate them for signs of stress or possible deception. Note their responses after they have finished speaking, or have a second SA take notes so that the primary interviewer can observe the interviewee.

At the conclusion of the interview, the facts should be recapped with the interviewee.

See Exhibit (400)-210.2 for the use of appropriate forms during TIGTA interviews.

210.6.1 Interview Notes. Complete notes are essential to effective investigating and reporting. Include the following in interview notes, as applicable:

- Case name and/or number;
- Date, time, and place of interview;
- Complete identification of the person interviewed, including position title or occupation, business or residential address, as appropriate, and contact information;
- Names of other persons present; and
- Summary of the interview.

Retain all notes (*e.g.*, handwritten, typed, etc.) and any audio and/or video recordings of all interviews. See Section 250.5.

210.7 Requests for Representation at Interviews.
An individual that is interviewed may request legal counsel or, if an IRS employee, NTEU representation.

210.7.1 Criminal Investigations. In any criminal investigation where the subject being interviewed requests legal representation, stop the interview to afford the person the opportunity to obtain counsel. If he/she later withdraws a request for legal representation, conduct the interview and indicate on Form OI 2028-M that the subject stated that he/she did not want counsel present in the interview.

If the SA is aware that the individual has obtained legal representation, refrain from any ex-parte communication with the individual without the consent or presence of the individual's counsel, unless the individual initiates communication with the SA, and the

right to legal representation is waived in writing by both the individual and the individual's counsel.

TIGTA procedures regarding ex-parte communication have been disseminated to bargaining unit employees and are available on the Internet at www.treas.gov/tigta/oi_interview.shtml, paragraph 18.

210.7.2 Non-Criminal and Non-Prosecution Investigations. The presence of legal counsel during an interview of the subject of a non-criminal or non-prosecution investigation is a privilege and not a right. Generally, the request for legal counsel will be granted unless counsel's presence will compromise the integrity of the investigation or impede the interview. If the request is granted, afford the employee a reasonable opportunity to obtain or consult with legal counsel. The interview will be deferred for this purpose, but not for an undue period of time.

If the SA believes the presence of legal counsel will impede or compromise the interview or investigation, the SA should consult with his/her ASAC, SAC, and/or the Operations Division, as appropriate. If denial of the presence of legal counsel is justified, inform the employee that TIGTA determined the presence of counsel was not deemed in the best interest of the Government. No other reason for the denial will be given. Thoroughly document cases where this privilege is not granted.

210.7.3 Attorney's Standing. Be aware of potential conflict of interest problems that might be present with certain attorneys, and take steps to have their presence denied, when appropriate. Counsel retained by an employee for presence during a TIGTA interview must be an attorney in good standing. Legal counsel cannot be an IRS or other Federal employee. See *Outside Activities and Employment* in IRS Document 12011, *Plain Talk About Ethics and Conduct*, codified in the Treasury Supplemental Standards of Ethical Conduct 5 CFR § 3101.106, and 18 U.S.C. § 205**.**

210.7.4 Non-Employee Requests for Counsel. A non-employee who is the subject of a non-criminal investigation or is a third-party witness has no right to counsel accorded by law. If the non-employee requests the presence of counsel or other representative at the interview, decide whether to conduct or discontinue the interview.

210.8 Role of Attorney or Representative in TIGTA Interviews.
In certain situations, NTEU representatives and private counsel may represent employees during an interview. Regardless of the situation, SAs are expected to control the interview. Representatives are expected to abide by professional standards and not disrupt the proceedings.

210.8.1 Private Attorneys. When the IRS employee being interviewed is accompanied by private counsel, in both criminal and non-criminal investigations, advise the attorney at the outset of the interview of the following:

- His/her function is strictly limited to giving advice to the employee;
- The proceeding is an interview, designed to gather facts and the employee's responses only;
- It is not a hearing; and
- If the IRS employee being interviewed is the subject of the investigation, both the employee and the attorney must sign Form OI 8115, Attorney Representation Agreement, when an interview involves the disclosure of information protected by 26 U.S.C. § 6103. See Section 210.9 regarding the disclosure of tax returns or tax return information to authorized legal representatives who are not IRS employees.

If the attorney refuses to abide by such limitations, the SA can consult with the ASAC, as appropriate, and resume or terminate the interview.

210.8.2 NTEU Representatives. The NTEU representative may clarify questions and answers, but may not answer questions for the employee. The employee must respond directly to questions. When a bargaining unit employee being interviewed is accompanied by an NTEU representative, in both criminal and non-criminal investigations, the role of the representative should generally be limited to:

- Clarifying the questions;
- Clarifying the answers;
- Assisting the employee in providing favorable or extenuating facts;
- Suggesting other employees who may have knowledge of relevant facts; and
- Advising the employee.

The role of the representative is not limited to the above. However, the NTEU representative may not transform the interview into an adversarial contest, as stated in IRS Document 11678, National Agreement Between IRS and NTEU, Article 5, Section 4F.

210.8.3 Disruption of Interview by NTEU Representative. If an NTEU representative does not abide by the general guidelines during an interview, take the following steps:

If...	Then...
The representative attempts to disrupt, unnecessarily delay, or interfere with the orderly progress of the interview, or attempts to turn the interview into an adversarial contest	Cite the National Agreement Between IRS and NTEU, including the provisions above, and ask the representative to conduct himself/herself within the confines of the agreement.

The representative continues to disrupt, delay, or interfere with the interview	Advise the employee that he/she must respond to questions and that the interview cannot continue with such disruption, delay, or interference.
Such activity does not cease	Remove the representative and consider whether to continue or terminate the interview, as appropriate.

Pursuant to the National Agreement Between IRS and NTEU, Article 5, Section 1C, in non-criminal investigations only, discussions between an NTEU representative and an employee are considered confidential by IRS.

210.9 Interviews Requiring Disclosure of Tax Returns or Return Information.
26 U.S.C. § 6103 prohibits disclosure of tax returns and tax return information except as authorized by the Internal Revenue Code. Certain sections of 26 U.S.C. § 6103 (*e.g.*, (k)(6) and (l)(4)) permit the disclosure of tax return information in connection with investigations or personnel matters. See Section 70 for more information on disclosure authority.

Interviews with employees may involve the discussion of tax returns or tax return information. Ensure that unauthorized disclosures do not occur in interviews with an employee who is accompanied by an authorized representative that is not an IRS employee.

For subject interviews where employees are accompanied by attorneys, obtain signatures from both the employee and the attorney on Form OI 8115, in order to disclose tax information under 26 U.S.C. § 6103(l)(4)(A). Form OI 8115 should not be used when interviewing IRS employees who are not subjects, such as witnesses or complainants. When interviewing employees in the presence of an authorized legal representative who is not an IRS employee without Form OI 8115, the employee should be cautioned prior to the interview not to disclose tax returns or return information in the presence of the representative.

210.10 Affidavits and Statements.
TIGTA reports must consist of facts supported by relevant evidence. Evidence may consist of affidavits or statements made to SAs by principals or third parties. These may be crucial in future hearings or court actions.

210.10.1 Authority to Take Affidavits. Questions may arise about an SA's authority to administer oaths or request information under oath. SAs may cite the sources shown in Chapter 200, General Management, Section 10.5 and Chapter 400, Section 10.2, of the TIGTA Operations Manual, or Treasury Order 115-01.

210.10.2 Affidavit. An affidavit is a written or printed declaration of facts made voluntarily, under oath, before an officer having authority to administer the oath. Preferably, the affidavit should be written by the affiant, in the words of the affiant. The affidavit should include only information relevant to the specific issue at hand. If a witness or subject declines to provide an affidavit, document this fact in the Form OI 2028-M.

210.10.3 Statement. A statement generally means the written declaration of matters of fact, without the affiant's oath, but properly signed and witnessed. The statement should include only information relevant to the specific issue at hand.

210.10.4 When to Take an Affidavit. The decision to request an affidavit must be based on the facts in the individual investigation. Attempt to secure an affidavit in any instance where statements by principals or third parties should be obtained in writing; however, consider consultation with the Assistant United States Attorney (AUSA) or appropriate prosecuting authority before taking an affidavit in a criminal case. An affidavit is recommended in the following situations:

- Where the person interviewed has made an oral admission, particularly where he/she is the principal or subject of the investigation;
- Confrontation-type interviews involving criminal matters where the subject or suspect agrees to an interview;
- Interviews of IRS employees in non-criminal investigations;
- Interviews of IRS employees in non-prosecution investigations;
- Where the person interviewed has information pertinent to the investigation, and there is reason to believe he/she may change or retract his/her oral statement; or
- To record the statement of a material witness, allowing the affiant to later refresh his/her memory if called to testify.

210.10.5 "Negative Statements" in Affidavits. At times, circumstances require OI to interview specific individuals and secure affidavits from them. In some instances, this requires taking "negative statements," (*i.e.*, statements from a witness that he/she did not do something or did not observe something with regard to an incident or allegation). Take a "negative statement" only to ensure that a witness will not change his/her testimony or create a fictitious story which differs from information furnished previously.

210.10.6 Affidavit Format. Use Form OI 2311, Affidavit, and Form OI 2311-A, Continuation Sheet, when practical. Consider the following when preparing an affidavit:

- The opening paragraph of an affidavit should clearly identify the affiant and the SA taking the affidavit;
- The concluding paragraph should show that the affiant read, understood, and voluntarily signed the affidavit without duress, reward, or promise of reward;

- One or more witnesses should attest to the signing of the affidavit by placing their signatures under the appropriate heading;
- The affidavit should contain only statements on matters directly bearing on the issues under investigation;
- Prepare separate affidavits when the affiant is relating criminal or ethics and conduct violations on the part of more than one individual;
- When an employee who is a witness is reluctant to furnish his/her residence address, instead insert his/her office address in the affidavit; and
- Prior to signing the affidavit, have the affiant sign each page and initial each correction and/or error.

210.10.7 Affidavits in Criminal Cases. In a criminal case, the affidavit should include, when applicable:

- That the affiant was advised of his/her rights; or
- That the affiant was assured that his/her truthful answers would not be used against him/her in a criminal prosecution, if prosecution was declined.

210.10.8 Special Situations. In some cases, the affiant may be unable to write or read the affidavit for him/herself, or other special circumstances may arise with regard to an affidavit. Use the following guidelines in handling special situations:

If...	Then...
The SA is required to write the affidavit for the individual	The full content of the affidavit should be read by the affiant prior to signing it.
The affiant declines to read it	The SA will read it to him/her.
The affiant is illiterate	The SA will read the contents of the affidavit to him/her in the presence of a witness. Note this fact on the last page of the affidavit.
An employee is interviewed and furnishes a signed affidavit or statement	Upon request, give him/her a copy of the signed affidavit or statement. Do not furnish a copy of an affidavit unless the affiant has signed it.
The witness wishes to retract or make a major change in an affidavit or statement which he/she has already submitted	Ask him/her to furnish a supplemental statement or affidavit.

210.10.9 Refusal to Sign Affidavit. In any case where the person interviewed voluntarily provided an affidavit or verbally dictated one to the SA, but then refuses to sign it, note such refusal on the affidavit and on the Form OI 2028-M documenting the interview. Also note any verbal confirmation regarding the accuracy of the affidavit if the SA reads the content to the individual.

210.10.10 Affidavits from Employee Complainants. Requesting affidavits from IRS employees who are complainants will depend on the circumstances. This may have an inhibiting effect upon employees bringing information to OI. If it is determined that the information should be supplied in writing, consider taking a statement rather than an affidavit, thereby eliminating the need for administering the oath, which might be inhibiting. Do not request an affidavit from an IRS employee complainant who has not waived confidentiality.

210.11 Question and Answer Statements.
Question and answer (Q&A) statements should be used only under circumstances where the use of a narrative affidavit or statement is clearly impractical. Q&A statements are a valuable investigative tool, particularly in interviewing principals. Q&A statements require careful, extensive preparation and the services of a reporter. Obtaining a Q&A statement may not be practical in most instances.

The purpose of the Q&A is to develop the facts in the case. Do not ask an employee personal questions if the information can be obtained through his/her personnel file. A statement of the witness' name and position at the beginning of the Q&A is sufficient in most cases.

All questions asked should be based on evidence or information in the investigator's possession. Investigators should not accuse an employee or non-employee of anything. Do not use a Q&A as an instrument for indulging in "fishing expeditions."

210.11.1 Authorization to Use Q&A. Seek authorization from the SAC prior to taking a Q&A statement from a principal or witness. The SAC is responsible for ensuring that the Q&A is properly initiated and conducted.

210.12 Recording Interviews.
Interviews conducted by OI may be electronically recorded (*e.g.,* audio, with or without video) by SAs in most circumstances. A “recorded interview” occurs when an SA, after notifying the interviewee of his/her official identity, electronically records the interviewee’s statement. A recorded interview may occur in a custodial or non-custodial situation. This section addresses overtly recording non-custodial interviews. See Section 210.20 for procedures for recording custodial interviews.

SAs must only use suitable recording equipment that has been approved by the Technical and Firearms Support Division (TFSD). No “dual use” equipment such as a

laptop computer, or any other device that is not designated as an electronic recording device, is permitted for use. TIGTA-issued cell phones and personally-owned equipment are not authorized to be used for recordings.

Prior to the decision to record any interview (except when mandated per Section 210.20), SAs should consider whether recording the interview is operationally prudent. Considerations may include: the preferences of the servicing AUSA, Federal and local laws and practices, the sufficiency of other evidence, whether prosecution is likely, the seriousness of the offense(s), whether an interviewee is likely to lie, and whether the interviewee's own words will controvert any doubt about the meaning, context, or voluntariness of their statement.

210.12.1 Documenting Recorded Interviews. After a recorded interview, prepare a Form OI 2028-M. The SA does not need to transcribe or extensively document the entire interview. Instead, summarize the recording and add the following caveat to the end of the Form OI 2028-M:

> "**Note:** The above is an interview summary and is not intended to be a verbatim account or complete memorialization of all statements made during the interview. Communications by the parties in the interview were electronically recorded, which captured the actual words spoken."

210.12.2 Handling Interview Recordings. The recordings of non-custodial interviews and victim or witness interviews should be considered for evidentiary value and treated as evidence, if appropriate. If the recording will be entered into evidence, the first download of the recording from the recording device will be directly to an individual digital media storage device (*e.g.*, DVD-R, CD-ROM). This original copy will be considered "best evidence" and will be preserved as evidence in accordance with Section 190.3. See Section 210.20 for recording requirements of custodial interviews.

All other recorded interviews not intended for use as evidence may be handled as investigative notes in accordance with Section 250.5.

210.12.3 Recording Employee Interviews. Interviews of employees may be electronically recorded (*e.g.*, audio, with or without video), by either party in most circumstances. However, the recording may not unreasonably delay the interview. An employee who chooses to record an interview must provide TIGTA personnel with advance notice so the SA can arrange for a recording by TIGTA as well. An employee cannot refuse to allow TIGTA to record an interview.

TIGTA procedures regarding recording of interviews have been disseminated to bargaining unit employees and are available on the Internet at www.treas.gov/tigta/oi_interview.shtml, paragraph 15.

The following are the procedures for recording an interview:

If...	Then...
OI records an interview	OI may furnish the employee a copy of the recording, if requested. Form OI 6501 must be documented to reflect a copy of the recording was provided to the interviewee.
The employee requests that the interview be recorded or is making his/her own recording	The SA will make a recording to maintain in OI records.

210.13 Interviews Involving Criminal Matters.
Generally, the subject of, or suspect in, a criminal investigation, either employee or non-employee, will not be interviewed unless the AUSA or an appropriate prosecuting official requests it, or agrees that such an interview is appropriate.

Do not rely solely on the admission of an accused person to corroborate or establish the violation of a law. Establish the violation of a law by developing evidence through the investigative process. Typically, the evidence should be secured prior to interviewing the subject or suspect. If this is not possible, independent evidence corroborating the admission should be obtained.

See Exhibit (400)-210.2 for use of appropriate forms during TIGTA interviews.

See Section 210.10 for obtaining affidavits.

210.14 Arranging Employee Interviews.
The amount of advance notice given to the employee to report for an interview will vary with the circumstances of the particular case. Absent safety or other specific investigative concerns, try to arrange the time and place of the interview so it will not unnecessarily inconvenience the employee or the employee's office. Whenever practical, ask the employee's supervisor to direct the employee to report for an interview.

210.14.1 Employee's Failure to Appear. If the employee fails to appear as requested for an interview in a non-criminal or non-prosecution case, ask the supervisory official to issue the employee a written order directing him/her to appear at the OI office, or other specified location, for an interview at a specified date and time to respond to questions. The written order should stipulate that the employee's failure to appear and respond to questions may subject him/her to "severe disciplinary action."

Consideration should be given whether to utilize such directives in criminal cases to avoid the potential perception of a custodial situation and/or non-voluntary statement.

210.15 Employee Refusal to Respond to Questioning.
Questions of official interest must be answered by employees who are being interviewed in non-criminal or non-prosecution investigations.

See Rules Concerning Employee Conduct and Official Activities in IRS Document 12011, *Plain Talk About Ethics and Conduct*, codified in Treasury Employee Rules of Conduct 31 CFR § 0.207.

210.15.1 Procedures. If an employee refuses to respond to questions during a non-criminal or non-prosecution interview, advise the employee as follows:

> Pursuant to IRS Document 12011, *Plain Talk About Ethics and Conduct*, codified in Treasury Employee Rules of Conduct 31 C.F.R. § 0.207, when directed by competent Treasury authority, employees must provide information, orally and/or in writing, and respond to questions in matters of official interest truthfully and under oath when required. Failure to respond as required may result in disciplinary action, including removal.

If it appears an employee still does not understand his/her obligation to respond to questions as set forth in the ethics and conduct rules, consider having the employee's supervisor issue the employee a written order to respond to TIGTA's questions, including the advisement that failure to respond may subject him/her to "severe disciplinary action."

Do not ask an employee why he/she refuses to answer questions. Since an employee has no right to refuse to answer questions in a non-criminal or non-prosecution investigation, any reasons provided are immaterial. Ask the employee at least two material questions relating to the matter under investigation to confirm that:

- The employee understands the seriousness of his/her refusal to respond to questions; and
- There is no misunderstanding about the employee's refusal to respond.

The questions asked and the answers expected should be related to "matters of official interest." Document the questions asked and the employee's actions or actual verbal responses at the time of refusal.

210.16 Warnings.
The United States Supreme Court held that if Federal employees are compelled to answer questions under the threat of losing their Federal Government employment, then the Federal Government may not use the employees' statements or any evidence

derived from those statements in any criminal prosecution. See *Garrity v. New Jersey,* 385 U.S. 493 (1967). Such statements are effectively "immunized."

When a Federal employee is interviewed during the course of a criminal investigation, SAs should provide the employee with an advisement of rights form that is designed to preserve the Government's ability to use the employee's statements by advising the employee that the interview is voluntary and that the employee will not be disciplined solely for refusing to answer questions. This is commonly referred to as the "Garrity" warning. The Garrity warning will be provided to all Federal employees using Form OI 5228-G, Waiver of Right to Remain Silent and of Right to Advice of Counsel (Miranda and Garrity Warning-Federal Employee), for custodial situations, or Form OI 5230, Non-Custodial Advisement of Rights (Garrity Warning), for non-custodial situations. See Section 210.17 and Section 210.18 for additional information.

In investigations where prosecution has been declined in lieu of administrative remedies, the Federal Government may compel the employee to answer questions. In such instances, the employee must be assured that his/her statements will not be used against the employee in any criminal proceeding. See *Kalkines v. United States* 472 F.2d 1391 (Ct. Cl. 1973). When an employee is compelled to answer questions, the SA will provide the employee with a warning form that is commonly referred to as a "Kalkines" warning. The Kalkines warning will be provided to the employee using Form OI 8112, Statement of Rights and Obligations (Kalkines Warning). If the employee refuses to answer questions when presented with the Kalkines warning, the employee may be terminated for that refusal. Any answer that the employee provides to SAs during the interview after a Kalkines warning has been provided, may be used for administrative purposes, but not for criminal prosecution. However, if an employee lies during a compelled interview, the employee may be prosecuted for false statements. See Section 210.17 and Section 210.18 for additional information.

In *Miranda v. Arizona,* 384 U.S. 436 (1966), the Supreme Court ruled that statements obtained from the custodial interrogation of a subject cannot be used at trial unless law enforcement officers advise him/her of specific rights and obtain a voluntary waiver of those rights. Failure to follow this "procedural safeguard," even for statements that are otherwise voluntary, can lead to suppression. Prior to the custodial interrogation, the subject must be advised of the following:

- He or she has the right to remain silent;
- That any statement he or she makes may be used as evidence against him or her;
- That he or she has a right to consult with an attorney and to have the attorney present during questioning; and
- That if he or she cannot afford an attorney, one will be appointed to represent him or her prior to questioning.

The Miranda decision is based on the premise that the Government can overcome a person's will (through compulsion) by more means than the use or threatened use of violence. The Miranda warning is an additional tool used to ensure that the subject's statements are voluntary when the subject is interrogated in a Government-dominated atmosphere. The Miranda warning will be provided to non-Federal employee subjects using OI Form 5228, Waiver of Right to Remain Silent and of Right to Advice of Counsel (Miranda Warning).

In any subject interview of a Federal employee in a criminal case, either the Garrity or Kalkines warning should be given. In custodial interviews of Federal employees, use OI Form 5228-G, which includes both the Miranda warning and the Garrity warning.

The Supreme Court, in the case of *NLRB v. J. Weingarten, Inc.* 420 U.S. 251 (1975), upheld a National Labor Relations Board (NLRB) decision that employees have a right to union representation at investigatory interviews. These rights have become known as the Weingarten rights. Weingarten rights will be provided to bargaining unit employee subjects of an investigation using IRS Form 8111, Employee Notification Regarding Union Representation, or IRS Form 9142, Employee Notification Regarding Third-Party Interviews, for bargaining unit third-party witnesses. See Section 210.17 for additional information.

210.17 Interviewing Bargaining Unit Employees.
Requirements for interviewing bargaining unit employees have been established by statute and case law. See TIGTA's investigatory interview procedures for bargaining unit employees available on the Internet at www.treas.gov/tigta/oi_interview.shtml.

The Civil Service Reform Act of 1978, Section 7114 (a)(2)(B) states, in part, the following: "An exclusive representative of an appropriate unit in an agency shall be given the opportunity to be represented at any examination of an employee in the unit by a representative of the agency in connection with an investigation if the employee reasonably believes that the examination may result in disciplinary action against the employee, and the employee requests such representation."

The Supreme Court has held that an Office of Inspector General is acting as a representative of the agency when interviewing bargaining unit employees, and therefore, a right to union representation exists.

See Section 210.10 for obtaining affidavits.

210.17.1 Contacting the Bargaining Unit Employee. Contact the employee's manager to schedule an interview with any bargaining unit employee unless there are specific investigative or safety concerns that would make such contact unwise.

When contacting the manager, advise the manager of the general subject matter of the interview, including whether the interview involves criminal or non-criminal issues, if known, and whether the employee is the subject of the investigation or a third-party witness.

If contacting the employee directly to schedule an interview, provide the employee the following information whenever practical:

- The general subject of the interview, including whether the interview involves criminal or non-criminal matters, if known, except when doing so would undermine the investigation;
- If he/she is the subject of an employee investigation or is being interviewed as a third-party witness;
- If the employee reasonably believes that the interview may result in disciplinary action, the employee is entitled to request union representation in the interview; and
- If the employee wishes to have union representation, the interview will be scheduled to allow the employee to seek representation, so long as it does not unduly delay the interview.

TIGTA procedures regarding contacting bargaining unit employees have been disseminated to bargaining unit employees and are available on the Internet at www.treas.gov/tigta/oi_interview.shtml, paragraphs 2 and 3.

210.17.2 Bargaining Unit Employee's Right to Union Representation. Under Federal law, bargaining unit employees have the right to request union representation at interviews in connection with an investigation if the employee reasonably believes that the interview may result in disciplinary action against him or her. This applies in criminal, non-criminal, and non-prosecution investigations.

Special consideration may be necessary to balance exigent circumstances (*e.g.,* safety or evidence preservation issues) with the right to union representation, such as in an ongoing workplace violence situation involving an immediate law enforcement response or a criminal act occurring in the presence of an SA. Document the circumstances in a Form OI 2028-M.

210.17.2.1 Representation by NTEU. Bargaining unit employees may only be represented by a person designated by the exclusively recognized labor organization for their bargaining unit, NTEU.

The NTEU does not have to furnish representation. If NTEU refuses to furnish representation, the employee may bring an attorney, or must attend the interview unaccompanied.

210.17.2.2 Representation Decision Chart. The following chart generally indicates a bargaining unit employee's options regarding representation during an interview, and OI's responses to those options.

If...	Then...
The employee, upon being advised of his/her right to union representation, states that he/she does not want a union representative present	Document the waiver of union representation in interview notes and on the Form OI 2028-M.
The employee requests representation	TIGTA may decline to conduct the interview or decide to conduct the interview with the representative present.
A decision is made to conduct the interview with the representative present	Give the employee reasonable time to get representation.
The interview proceeds without representation and the employee believes that disciplinary action may result because the subject matter of the interview changes	The employee may request a brief delay to request representation.
An employee is represented and the subject matter of the interview changes to a matter the representative and the employee have not discussed	If requested, allow the representative and the employee a brief recess to confer on the new issue.
The employee waives his/her right to union representation and requests private counsel	Generally, allow counsel in the interview, unless there is a compelling reason not to. If there are concerns regarding the presence of counsel in the interview, refer the request to the ASAC, SAC, and/or Operations Division, as appropriate, to determine whether the attorney will be allowed at the interview (See Section 210.7).

210.17.3 Criminal Investigation. When an investigation results in evidence that a Federal law has been violated by a bargaining unit employee, present the facts of the case to an AUSA or other appropriate DOJ attorney. Secure a decision regarding prosecution and whether the employee should be interviewed.

Note: If the matter under investigation by TIGTA is not a Federal crime, or no evidence supports a violation of Federal law, the SA should not seek, and has no authority to obtain, a declination from the United States Attorney's Office (USAO). See Chapter 700, Section 70.5.1.1 for the referral process and requirements to another law enforcement agency or the State/local prosecutor.

210.17.3.1 Interviewing Bargaining Unit Employee as Subject of Criminal Investigation. If the employee is to be interviewed, whenever practical (absent exigent circumstances such as an ongoing workplace violence situation), inform the employee of the following at the beginning of the interview:

- He/she is the subject of an official investigation;
- The general nature of the allegations against him/her and that the allegations are criminal in nature;
- His/her rights as stated on Form OI 5228-G, if the employee is in custody, or on Form OI 5230, if the employee is not in custody. If the employee waives his/her rights, then obtain the employee's acknowledgement signature on Form OI 5228-G or Form OI 5230 and provide the employee a copy of the signed form. See Section 210.20 for additional procedures on interviewing a person in custody;
- His/her right to union representation by providing the employee with IRS Form 8111. Ask the employee to acknowledge receipt of the notification by signing IRS Form 8111, and provide the employee with a copy of the signed form. Give the employee a reasonable amount of time to secure union representation, if requested. See Section 210.17.2 for bargaining unit employees' right to union representation; and
- Place the employee under oath or affirmation by having the employee swear or affirm that his/her testimony will be true, under penalty of perjury.

At the conclusion of the interview, recap the employee's testimony and document the facts in a Form OI 2028-M. Unless otherwise directed by an AUSA, offer the subject the opportunity to complete an affidavit. Document either that the affidavit was declined by the subject or that it is attached to the Form OI 2028-M.

See Exhibit (400)-210.2 for use of appropriate forms during TIGTA interviews.

210.17.3.2 Documentation of Rights and Oath/Affirmation. Document the following, as applicable, in the opening portion of a Form OI 2028-M, statement, or affidavit:

- The issuance of Form OI 5228-G or Form OI 5230;
- The issuance of IRS Form 8111, and whether the employee waives presence of union representation;
- The general nature of any exigent circumstances;
- Any witnesses present; and

- The employee was placed under oath or affirmation, as appropriate.

210.17.4 Non-Prosecution Investigation. When an investigation results in evidence that a Federal law has been violated by a bargaining unit employee and prosecution has been declined by an AUSA or other DOJ attorney, or the violation is subject to a blanket declination agreement approved by the appropriate DOJ attorney, discuss the facts of the investigation with the ASAC, SAC, and/or Operations Division, as appropriate, to determine whether the employee is to be interviewed.

210.17.4.1 Interviewing a Bargaining Unit Employee as the Subject of Non-Prosecution Investigation. If the employee is to be interviewed, at the beginning of the interview, inform the employee of the following:

- He/she is the subject of an official investigation;
- The general nature of the allegations against him/her and that the allegations constitute violations of Federal criminal law;
- Prosecution has been declined and his/her rights as stated on Form OI 8112. Ask the employee to acknowledge receipt of the assurance by signing Form OI 8112 and give him/her a copy of the signed form. After being advised that prosecution has been declined, a bargaining unit employee accompanied by a union representative may request a reasonable delay of the interview;
- His/her right to union representation by providing the employee IRS Form 8111. Ask the employee to acknowledge receipt of the notification by signing IRS Form 8111 and provide the employee a copy of the signed form. Give the employee a reasonable amount of time to secure union representation, if requested. See Section 210.17.2 regarding bargaining unit employee's right to union representation; and
- The Privacy Act provisions by providing the employee a copy of Privacy Act Notice 417 and explaining the provisions of the notice to the employee.
- Place the employee under oath or affirmation by having the employee swear or affirm that his/her testimony will be true, under penalty of perjury.

TIGTA procedures regarding the use of Form OI 8112 have been disseminated to bargaining unit employees and are available on the Internet at http://www.treas.gov/tigta/oi_interview.shtml, paragraphs 12 and 14.

During the interview, if the employee makes statements that:

- Indicate he/she has committed a criminal offense;
- The nature or extent of which was previously unknown to the interviewing SA and has not been discussed with an AUSA; and,
- Referral for prosecution appears likely; then
    - Provide the employee his/her rights as stated on Form OI 5230.

- If the employee waives his/her rights, obtain the employee's acknowledgement signature on Form OI 5230, provide the employee a copy of the signed form, and continue the interview as appropriate.

At the conclusion of the interview, recap the employee's testimony and document the facts in a Form OI 2028-M. Offer the subject the opportunity to complete an affidavit. Document either that the affidavit was declined by the subject or that it is attached to the Form OI 2028-M.

See Exhibit (400)-210.2 for use of appropriate forms during TIGTA interviews.

210.17.4.2 Documentation of Rights and Oath/Affirmation. Document the following, as applicable, in the opening portion of a Form OI 2028-M, statement, or affidavit:

- The issuance of Form OI 8112;
- The issuance of IRS Form 8111, and whether the employee waives presence of union representation;
- The issuance of Privacy Act Notice 417;
- Any witnesses present;
- The employee was placed under oath or affirmation, as appropriate; and
- The issuance of Form OI 5230, if it became applicable.

210.17.5 Non-Criminal Investigation. When an investigation results in evidence that a bargaining unit employee has committed acts of misconduct that do not constitute violations of Federal criminal law, discuss the facts of the case with the ASAC, SAC, and/or Operations, as appropriate, to determine whether the employee is to be interviewed.

210.17.5.1 Interviewing a Bargaining Unit Employee as Subject of Non-Criminal Investigation. If the employee is to be interviewed, whenever practical (absent exigent circumstances such as an ongoing workplace violence situation), inform the employee of the following at the beginning of the interview:

- He/she is the subject of an official investigation;
- The general nature of the allegations against him/her and that the allegations are administrative in nature (*e.g.*, constitute violations of ethics and conduct rules);
- His/her right to union representation by providing the employee with IRS Form 8111. Ask the employee to acknowledge receipt of the notification by signing IRS Form 8111, and provide the employee with a copy of the signed form. Give the employee a reasonable amount of time to secure union representation, if requested. See Section 210.17.2 regarding bargaining unit employees' right to union representation; and
- The Privacy Act provisions by providing the employee with a copy of Privacy Act Notice 417 and explaining the provisions of the notice to the employee.

- Place the employee under oath or affirmation by having the employee swear or affirm that his/her testimony will be true, under penalty of perjury.

During the interview, if the employee makes statements that:

- Indicate he/she has committed a criminal offense;
- The nature or extent of which was previously unknown to the interviewing SA and has not been discussed with an AUSA; and
- Referral for prosecution appears likely, then
  - Provide the employee with his/her rights by providing Form OI 5230.
  - If the employee waives his/her rights, obtain the employee's acknowledgement signature on Form OI 5230, and provide the employee a copy of the signed form, and continue the interview as appropriate.

At the conclusion of the interview, recap the employee's testimony and document the facts in a Form OI 2028-M. Offer the subject the opportunity to complete an affidavit. Document either that the affidavit was declined by the subject or that it is attached to the Form OI 2028-M.

See Exhibit (400)-210.2 for use of appropriate forms during TIGTA interviews.

210.17.5.2 Documentation of Rights and Oath/Affirmation. Document the following, as applicable, in the opening portion of a Form OI 2028-M, statement, or affidavit:

- The issuance of IRS Form 8111, and whether the employee waives presence of union representation;
- The issuance of Privacy Act Notice 417;
- The general nature of any exigent circumstances;
- Any witnesses present;
- The employee was placed under oath or affirmation, as appropriate; and
- The issuance of Form OI 5230, if it became applicable.

210.17.6 Interviewing Bargaining Unit Employees as Third-Party Witnesses. Bargaining unit employees who are third-party witnesses are entitled to union representation if they reasonably believe the interview may result in disciplinary action. Whenever practical, inform the employee of the following at the beginning of the interview:

- He/she will be interviewed as a third-party witness in an official investigation;
- His/her notification as a bargaining unit employee regarding third-party interviews, as stated on IRS Form 9142;
- Ask the employee to acknowledge receipt of IRS Form 9142 by signing the form and give the employee a copy of the signed form.

  - Some circumstances could warrant verbal advisement in the absence of Form 9142.
  - If the employee, after having been provided the subject matter of the interview, reasonably believes he/she may be subject to discipline for his/her statements and asks for union representation, consider whether to grant the request or to discontinue the interview.
  - If the interview is to be continued, allow the employee a reasonable amount of time to obtain union representation.
- If the complaint or investigation is administrative (non-criminal or non-prosecution) at the time of the third-party interview, inform the employee witness of the Privacy Act provisions by providing the employee with a copy of Privacy Act Notice 417, Employee Interview, and explain the provisions of the notice to the employee; and
- Place the employee under oath or affirmation by having the employee swear or affirm that his/her testimony will be true, under penalty of perjury.

Note: There may be situations involving urgent or particularly sensitive circumstances where administering an oath is not appropriate. SAs should use discretion and sound judgement in such circumstances.

Interviews initiated by an employee/complainant will not normally require union representation. However, if the complainant furnishes information that the SA reasonably believes may result in disciplinary action to the complainant, the complainant should be advised of his/her right to union representation as stated on IRS Form 8111 or 9142.

During the interview, if the employee makes statements that:

- Indicate he/she has committed a criminal offense;
- The nature or extent of which was previously unknown to the interviewing SA and has not been discussed with an AUSA; and,
- Referral for prosecution appears likely, then
  - Provide the employee his/her rights as stated on Form OI 5230.
  - If the employee waives his/her rights, obtain the employee's acknowledgement signature on Form OI 5230, provide the employee a copy of the signed form, and continue the interview as appropriate.

At the conclusion of the interview, recap the witness' testimony and document the facts in a Form OI 2028-M.

See Exhibit (400)-210.2 for guidance on appropriate forms to provide during TIGTA interviews.

210.17.6.1 Documentation of Rights and Oath/Affirmation. Document the following, as applicable, in the opening portion of a Form OI 2028-M, statement, or affidavit:

- The issuance of IRS Form 9142 or verbal advisement of such when necessary;
- In administrative (non-criminal or non-prosecution) complaints and investigations, the issuance of Privacy Act Notice 417 to the employee witness;
- Document the Form OI 2028-M if the witness requests and is granted confidentiality. See 210.2.5.
- The employee was placed under oath or affirmation, as appropriate; and
- The issuance of Form OI 5230, if it became applicable.

210.18 Interviewing Non-Bargaining Unit Employees.
Non-bargaining unit employees are not entitled to union representation during TIGTA interviews.

See Section 210.10 for obtaining affidavits.

210.18.1 Criminal Investigation. When an investigation results in evidence that a Federal law has been violated by a non-bargaining unit employee, present the facts of the case to an AUSA or other appropriate DOJ attorney. Secure a decision regarding prosecution and whether the employee should be interviewed.

Note: If the matter under investigation by TIGTA is not a Federal crime, or no evidence supports a violation of Federal law, the SA should not seek, and has no authority to obtain, a declination from the USAO. See Chapter 700, Section 70.5.1.1 for the referral process and requirements to another law enforcement agency or the State/local prosecutor.
210.18.1.1 Interviewing Non-Bargaining Unit Employee as Subject of Criminal Investigation. If the employee is to be interviewed, whenever practical, inform the employee of the following at the beginning of the interview:

- He/she is the subject of an official investigation;
- The general nature of the allegations against him/her are criminal in nature;
- If the employee elects to waive his/her rights, then obtain the employee's acknowledgement signature on Form OI 5228-G, if the employee is in custody or Form OI 5230, if the employee is not in custody. Provide the employee with a copy of the signed form. See Section 210.20 for additional procedures on interviewing persons in custody; and
- If the employee waives his/her rights, place the employee under oath or affirmation by having the employee swear or affirm that his/her testimony will be true, under penalty of perjury.

At the conclusion of the interview, recap the employee's testimony and document the facts in a Form OI 2028-M. Unless otherwise directed by an AUSA, offer the subject the opportunity to complete an affidavit. Document either that the affidavit was declined by the subject or that it is attached to the Form OI 2028-M.

See Exhibit (400)-210.2 for use of appropriate forms during TIGTA interviews.

210.18.1.2 Documentation of Rights and Oath/Affirmation. Document the following, as applicable, in the opening portion of a Form OI 2028-M, statement, or affidavit:

- The issuance of Form OI 5228-G or Form OI 5230;
- Any witnesses present; and
- The employee was placed under oath or affirmation, as appropriate.

210.18.2 Non-Prosecution Investigation. When an investigation results in evidence that a Federal law has been violated by a non-bargaining unit employee and prosecution has been declined by an AUSA or other DOJ attorney, or the violation is subject to a blanket declination agreement approved by the appropriate DOJ attorney, discuss the facts of the investigation with the ASAC, SAC, and/or Operations Division, as appropriate, to determine whether the employee is to be interviewed.

210.18.2.1 Interviewing Non-Bargaining Unit Employee as Subject of Non-Prosecution Investigation. If the employee is to be interviewed, at the beginning of the interview, inform the employee of the following:

- He/she is the subject of an official investigation;
- The general nature of the allegations against him/her and that the allegations constitute violations of Federal criminal law;
- Prosecution has been declined and his/her rights as stated on Form OI 8112. Ask the employee to acknowledge receipt of the assurance by signing Form OI 8112 and give him/her a copy of the signed form;
- If union representation is requested, inform the employee that a non-bargaining unit employee is not entitled to union representation;
- The Privacy Act provisions by providing the employee a copy of Privacy Act Notice 417 and explaining the provisions of the notice to the employee; and
- Place the employee under oath or affirmation by having the employee swear or affirm that his/her testimony will be true, under penalty of perjury.

During the interview, if the employee makes statements that:

- Indicate he/she has committed a criminal offense;
- The nature or extent of which was previously unknown to the interviewing SA and has not been discussed with an AUSA; and,

- Referral for prosecution appears likely, then
  - Provide the employee his/her rights as stated on Form OI 5230.
  - If the employee waives his/her rights, obtain the employee's acknowledgement signature on Form OI 5230, provide the employee a copy of the signed form, and continue the interview as appropriate.

At the conclusion of the interview, recap the employee's testimony and document the facts in a Form OI 2028-M. Offer the subject the opportunity to complete an affidavit. Document either that the affidavit was declined by the subject or that it is attached to the Form OI 2028-M.

See Exhibit (400)-210.2 for guidance on appropriate forms to provide during TIGTA interviews.

210.18.2.2 Documentation of Rights and Oath/Affirmation. Document the following, as applicable, in the opening portion of a Form OI 2028-M, statement, or affidavit:

- The issuance of Form OI 8112;
- The issuance of Privacy Act Notice 417;
- Any witnesses present;
- The employee was placed under oath or affirmation, as appropriate; and
- The issuance of Form OI 5230, if it became applicable.

210.18.3 Non-Criminal Investigation. When an investigation results in evidence that a non-bargaining unit employee has committed acts of misconduct that do not constitute violations of Federal criminal laws, discuss the facts of the case with the ASAC, SAC, and/or Operations Division, as appropriate, to determine whether the employee is to be interviewed.

210.18.3.1 Interviewing Non-Bargaining Unit Employee as Subject of Non-Criminal Investigation. Whenever practical, inform the employee of the following at the beginning of the interview:

- That he/she is the subject of an official investigation;
- The general nature of the allegations against him/her and that the allegations are administrative in nature (*e.g.*, constitute violations of ethics and conduct rules);
- The Privacy Act provisions by providing the employee with a copy of Privacy Act Notice 417 and explaining the provisions of the notice to the employee; and
- Place the employees under oath or affirmation by having the employee swear or affirm that his/her testimony will be true, under penalty of perjury.

See Exhibit (400)-210.2 for use of appropriate forms during TIGTA interviews.

During the interview, if the employee makes statements that:

- Indicate he/she has committed a criminal offense;
- The nature or extent of which was previously unknown to the interviewing SA and has not been discussed with an AUSA; and,
- Referral for prosecution appears likely, then
    - Provide the employee his/her rights as stated on Form OI 5230.
    - If the employee waives his/her rights, obtain the employee's acknowledgement signature on Form OI 5230, provide the employee a copy of the signed form, and continue the interview as appropriate.

At the conclusion of the interview, recap the employee's testimony and document the facts in a Form OI 2028-M. Offer the subject the opportunity to complete an affidavit. Document either that the affidavit was declined by the subject or that it is attached to the Form OI 2028-M.

210.18.3.2 Documentation of Rights and Oath/Affirmation. Document the following, as applicable, in the opening portion of a Form OI 2028-M, statement, or affidavit:

- The issuance of Privacy Act Notice 417;
- Any witnesses present;
- The employee was placed under oath or affirmation, as appropriate; and
- The issuance of Form OI 5230, if it became applicable.

210.18.4 Interviewing Non-Bargaining Unit Employee as Third-Party Witness. Whenever practical, inform a non-bargaining unit employee of the following at the beginning of the interview:

- He/she will be interviewed as a third-party witness in an official investigation; and
- If the employee requests union representation, or inquires about his/her right to representation, that he/she is not entitled to union representation because he/she is not a bargaining unit employee;
- If the complaint or investigation is administrative (non-criminal or non-prosecution) at the time of the third-party interview, inform the employee witness of the Privacy Act provisions by providing the employee with a copy of the Privacy Act Notice 417, and explain the provisions of the notice to the employee; and
- Place the employee under oath or affirmation by having the employee swear or affirm that his/her testimony will be true, under penalty of perjury.

Note: There may be situations involving urgent or particularly sensitive circumstances where administering an oath is not appropriate. SAs should use discretion and sound judgement in such circumstances.

During the interview, if the employee makes statements that:

- Indicate he/she has committed a criminal offense;
- The nature or extent of which was previously unknown to the interviewing SA and has not been discussed with an AUSA; and
- Referral for prosecution appears likely, then
  - Provide the employee with his/her rights as stated on Form OI 5230.
  - If the employee waives his/her rights, obtain the employee's acknowledgement signature on Form OI 5230, provide the employee a copy of the signed form, and continue the interview as appropriate.

At the conclusion of the interview, recap the witness' testimony and document the facts in a Form OI 2028-M.

210.18.4.1 Documentation of Rights and Oath/Affirmation. Document the following, as applicable, in the opening portion of a Form OI 2028-M, statement, or affidavit:

- In administrative (non-criminal or non-prosecution) complaints or investigations, the issuance of Privacy Act Notice 417 to the employee witness;
- Document the Form OI 2028-M if the witness requests and is granted confidentiality. (See 210.2.5);
- The employee was placed under oath or affirmation, as appropriate; and
- The issuance of Form OI 5230, if it became applicable.

210.19 Interviewing Non-Employees.
Non-employees are interviewed as complainants, witnesses, informants, or subjects of investigations. They have no obligation to respond to questions. When a non-employee requests the presence of legal counsel or other representative at a third-party or non-criminal interview, decide whether to conduct or discontinue the interview.

See Section 210.10 for obtaining affidavits.

210.19.1 Criminal Investigation. When an investigation results in evidence that a Federal law has been violated by a non-employee, present the facts of the case to an AUSA or other appropriate DOJ attorney. Secure a decision regarding prosecution and whether the non-employee should be interviewed.

Note: If the matter under investigation by TIGTA is not a Federal crime, or no evidence supports a violation of Federal law, the SA should not seek, and has no authority to obtain, a declination from the USAO. See Chapter 700, Section 70.5.1.1 for the referral process and requirements to another law enforcement agency or the State/local prosecutor.

210.19.1.1 Interviewing Non-Employee as the Subject of a Criminal Investigation. If the non-employee is to be interviewed, inform the non-employee of the following at the beginning of the interview:

- He/she is being interviewed in an official investigation; and
- If in custody, his/her rights as stated on Form OI 5228. If the non-employee elects to waive his/her rights, then obtain the non-employee's acknowledgment signature on Form OI 5228.

Note: If the subject of the criminal investigation is a non-IRS employee, but is a current Federal Government employee of another Agency, he/she must be provided with Form OI 5228-G, if in custody, or Form OI 5230, if not in custody to ensure the Garrity warning is provided.

Consider the benefit of interviewing the non-employee under oath or affirmation. If applicable, place the individual under oath or affirmation by having him/her swear or affirm that his/her testimony will be true, under penalty of perjury.

At the conclusion of the interview, recap the non-employee's testimony and document the facts in a Form OI 2028-M. Unless otherwise directed by an AUSA, offer the subject the opportunity to complete an affidavit. Document either that the affidavit was declined by the subject or that it is attached to the Form OI 2028-M.

See Exhibit (400)-210.2 for use of appropriate forms during TIGTA interviews.

210.19.1.2 Documentation of Rights and Oath/Affirmation. Document the following, as applicable, in the opening portion of a Form OI 2028-M, statement, or affidavit:

- The issuance of Form OI 5228, if provided;
- Any witnesses present; and
- If the non-employee was placed under oath or affirmation.

210.19.2 Non-Prosecution Investigation. When an investigation results in evidence that a Federal law has been violated by a non-employee and prosecution has been declined by an AUSA or other DOJ attorney, or the violation is subject to a blanket declination agreement approved by the appropriate DOJ attorney, discuss the facts of the investigation with the ASAC, SAC, and/or Operations Division, as appropriate, to determine whether the non-employee is to be interviewed.

210.19.2.1 Interviewing Non-Employee as Subject of Non-Prosecution Investigation. If the non-employee is to be interviewed, when practical inform the non-employee of the following at the beginning of the interview:

- He/she is being interviewed in an official investigation;

- The Privacy Act provisions by providing the appropriate Privacy Act Notice (416 or 425) and explaining the notice to him/her; and
- Consider the benefit of interviewing the non-employee under oath or affirmation. If applicable, place the individual under oath or affirmation by having him/her swear or affirm that his/her testimony will be true, under penalty of perjury.

At the conclusion of the interview, recap the non-employee's testimony and document the facts in a Form OI 2028-M. Offer the subject the opportunity to complete an affidavit. Document either that the affidavit was declined by the subject or that it is attached to the Form OI 2028-M.

See Exhibit (400)-210.2 for use of appropriate forms during TIGTA interviews.

210.19.2.2 Documentation of Notice and Oath/Affirmation. Document the following, as applicable, in the opening portion of a Form OI 2028-M, statement, or affidavit:

- The issuance of the applicable Privacy Act Notice;
- Any witnesses present; and
- If the non-employee was placed under oath or affirmation.

210.19.3 Non-Criminal Investigation. When an investigation results in evidence that a non-employee has committed acts that do not constitute violations of Federal criminal law, discuss the facts of the case with the ASAC, SAC, and/or Operations Division, as appropriate, to determine whether the non-employee is to be interviewed.
210.19.3.1 Interviewing Non-Employee as Subject of a Non-Criminal Investigation. If the non-employee is to be interviewed, when practical inform the non-employee of the following at the beginning of the interview:

- He/she is being interviewed in an official investigation;
- The Privacy Act provisions by providing the appropriate Privacy Act Notice (416 or 425) and explaining the notice to him/her; and
- Consider the benefit of interviewing the non-employee under oath or affirmation. If applicable, place the individual under oath or affirmation by having him/her swear or affirm that his/her testimony will be true, under penalty of perjury.

At the conclusion of the interview, recap the employee's testimony and document the facts in a Form OI 2028-M. Offer the subject the opportunity to complete an affidavit. Document either that the affidavit was declined by the subject or that it is attached to the Form OI 2028-M.

See Exhibit (400)-210.2 for use of appropriate forms during TIGTA interviews.

210.19.3.2 Documentation of Notice and Oath/Affirmation. Document the following, as applicable, in the opening portion of a Form OI 2028-M, statement, or affidavit:

- The issuance of the Privacy Act Notice;
- Any witnesses present; and
- If the non-employee was placed under oath or affirmation.

210.19.4 Interviewing a Non-Employee as a Third-Party Witness. Advise the non-employee that he/she is to be interviewed as a third-party witness in an official investigation. If the complaint or investigation is administrative (non-criminal or non-prosecution) at the time of the third-party interview, advise the non-employee of the Privacy Act provisions by providing the appropriate Privacy Act Notice (416 or 425) and explaining the notice to him/her. See Section 210.2.5.

At the conclusion of the interview, recap the witness' testimony and document the facts in a Form OI 2028-M.

Document Form OI 2028-M for issuance of the Privacy Act Notice if it was applicable. Document the Form OI 2028-M if the witness requests and is granted confidentiality.

210.20 Custodial Interviews.
If a subject is in custody or is deprived of his/her freedom of action in any significant way, advise the subject of his/her Miranda rights as stated on Form OI 5228 or similar format. Current Federal employees should be provided with both the Miranda warning and the Garrity warning in custodial interviews. Provide Federal employee subjects in custody with Form OI 5228-G, which includes both the Miranda and Garrity warnings. Advising a person of his/her rights in a custodial situation is essential to protect the admissibility, as evidence, of any information, statement, or affidavit provided by the person. In the opening portion of the statement or affidavit, include a statement that such advisement was given to the subject. If given verbally with no written statement or affidavit, document the fact on Form OI 2028-M that the advice of rights was given and identify any witnesses who were present.

Obtain a written waiver if the subject elects to waive the right to counsel and the right to remain silent. Use TIGTA Form OI 5228, Form OI 5228-G, or similar wording, as appropriate. If circumstances make it impossible to obtain a signed Form OI 5228 or 5228-G (waiver), a verbal waiver may be accepted, provided it is witnessed by another SA or other credible person. Due caution should be exercised if proceeding without a signed waiver.

TIGTA procedures regarding custodial interviews of IRS employees have been disseminated to bargaining unit employees and are available on the Internet at www.treasury.gov/tigta/oi_interview.shtml, paragraph 10.

See Section 210.10 for obtaining affidavits.

210.20.1 Recording Custodial Interviews. This policy establishes a presumption that the custodial statement of an individual in a place of detention with suitable recording equipment, following arrest but prior to initial appearance, will be electronically recorded, subject to the limited exceptions described in Section 210.20.1.3 below.

210.20.1.1 Requirements. The policy to record in-custody statements applies when the following factors exist:

- Custody, Timing, and Jurisdiction. This policy applies to the subjects of TIGTA investigations, after their arrest for a Federal crime, but prior to their initial court appearance before a judicial officer under Federal Rule of Criminal Procedure 5. Interviews in non-custodial settings are excluded from this policy.

- Place of Detention. The policy applies when the subject is held in a place of detention. A place of detention is any structure where persons are held in connection with Federal criminal charges and can be interviewed. A place of detention includes any TIGTA office, other Federal facilities, and any State, local, or tribal law enforcement facility, office, correctional or detention facility, jail, police or sheriff's station, holding cell, or other structure used for such purpose.

  Recording under this policy is not required while a person is waiting for transportation, or is en route, to a place of detention. However, no supervisory approval is needed if an agent deems it prudent or necessary to record a post-arrest custodial interview while awaiting transportation or en route to a place of detention.

- Suitable Recording Equipment. This policy applies when the place of detention or the agent has suitable recording equipment. Use only suitable recording equipment that has been approved by the Technical and Firearms Support Division (TFSD). In order to avoid potential disclosure issues, TIGTA will use its own recording equipment and must ensure that non-TIGTA recording equipment at the "place of detention" is turned off.

  TIGTA-issued cell phones or personally-owned equipment will not be used for recordings. No "dual use" equipment, such as tablets and laptop computers, or any other device that is not designated as an electronic recording device is permitted for use.

There is no requirement that interviews not meeting the above criteria be recorded; however, agents are encouraged to consider electronic recording in other interviews, in accordance with TIGTA policy and consultation with a prosecutor.

210.20.1.2 Procedures for Recording Custodial Interviews. Recording under this policy may be covert or overt. Covert recording constitutes consensual monitoring, which is allowed by Federal law. See 18 U.S.C. 2511(2)(c). Covert recording of custodial subject interviews per this policy may be executed without constraint by the procedures prescribed by other TIGTA policies for consensual monitoring, *i.e.*, supervisory approval and TIGTA Form OI 5177 is not required. The decision to covertly record the interview should be discussed with the SA's supervisor and the prosecutor, prior to arrest.

The electronic recording must begin as soon as the subject enters the interview area and will continue until the interview is completed. When overtly recording, the SA will start the recording with a preamble that provides the date, time, and participants, as well as a reading (or re-reading if previously read) of the interviewee's Miranda rights, followed by the interviewee's acknowledgment and waiver of these rights as is practical. In instances where the recording is conducted covertly, the preamble will be recorded outside the presence of the interviewee and as contemporaneously with the start of the interview as is practical. The covert recording should also address the interviewee's Miranda rights in the same manner as is described above for overt recordings. In both overt and covert recordings, ensure Federal employee subjects are also advised of the Garrity warning as stated on Form OI 5228-G. In addition, IRS bargaining unit employee subjects are to be notified of their right to union representation via IRS Form 8111.

The electronic recording of the interview may be audio only, or both audio and video, if available.

The recordings of custodial subject interviews per this policy will be treated as evidence. The first download of the recording from the digital recording device will be directly to an individual digital media storage device (*e.g.,* DVD-R, CD-ROM). This original copy will be considered "best evidence" and will be preserved as evidence in accordance with Section 190.3.

Audio recordings of interviews not within the scope of this section or outlined within section 210.12.2 are not necessarily treated as evidence, but as investigative notes in accordance with Section 250.5.

210.20.1.3 Exceptions to Mandatory Recording of Post-Arrest Custodial Interviews. A decision not to record an interview that would otherwise presumptively be recorded under this policy must be documented by the agent on a separate document (*e.g.,* letterhead memorandum) and made available to, or provided to, the United States Attorney's Office. Exceptions to the presumption of recording are:

- Refusal by the interviewee. If the interviewee is informed that the interview will be recorded and indicates that he or she is willing to give a statement but only if it

is not electronically recorded, then a recording need not take place. Additionally, if the interviewee asks to stop a recording that has already been started but agrees to continue the interview, the agent may cease recording while continuing the interview;
- Public Safety and National Security Exception. There is no presumption of electronic recording where questioning is done for the purpose of gathering public safety information under *New York v. Quarles*. The presumption of recording likewise does not apply to those limited circumstances where questioning is undertaken to gather national security-related intelligence or questioning concerning intelligence, sources, or methods, the public disclosure of which would cause damage to national security;
- Recording is not reasonably practicable. Circumstances may prevent, or render impracticable, the recording of an interview, such as equipment malfunction, an unexpected need to move the interview, or too many interviews to record with available equipment in a limited timeframe; and
- Residual exception. The SAC and the United States Attorney, or their designees, agree that a significant and articulable law enforcement purpose (*e.g.,* avoiding disclosure of a sensitive law enforcement technique) requires the interview not be recorded.

210.20.1.4 Documenting Recorded Interviews. After the interview, prepare a Form OI 2028-M. The agent need not transcribe or extensively document the entire interview. Instead, summarize the recording and add the following caveat or similar wording to the end of the Form OI 2028-M:

> "**Note:** The above is an interview summary and not a verbatim account or complete memorialization of all statements made during the interview. Communications by the parties in the interview were electronically recorded, which captured the actual words spoken."

210.20.2 Special Custodial Interview Considerations. TIGTA agents may encounter situations in which a subject of a non-criminal/non-prosecution case, or a witness in any type of case, is already in the custody of another agency. Such individuals are not necessarily in "custody" for TIGTA purposes. Prior to conducting the interview:

- Determine if it is necessary to conduct the interview by consulting with the ASAC, SAC, Operations Division, and/or prosecuting official, as appropriate. For example, the subject of a TIGTA non-criminal post appointment arrest investigation, who is in custody pending trial, can essentially only be asked to confirm the arrest and charges; therefore, an interview of that subject in custody may not be appropriate; and
- Determine if the interviewee is considered in custody for TIGTA purposes, by consulting with the ASAC, SAC, Operations Division, Counsel, and/or prosecuting official, as appropriate. This custodial determination governs which

forms must be provided; therefore, consideration should be made regarding employee forms which compel the employee to answer questions.

210.21 Interviewing Minors.
As a general rule, avoid interviewing minors as witnesses whenever possible. However, circumstances may arise which will require an interview of a minor.

210.20.1 Minors. Each Federal court accepts the State law and procedure for the jurisdiction where the court is located when considering the testimony of a minor. Anyone under 21 years of age should be considered as a possible minor, because the age of maturity, legal rights, responsibilities, and protection of minors may vary from State to State.

Protect a minor's special rights and status as defined in each State's law. Any subject or suspect in custody must be advised of his/her Miranda rights.

210.21.2 Parental Approval. Consider the following when interviewing a minor:

- A parent or guardian should be present, or should extend permission to conduct the interview of persons under 18 years of age;
- Parental presence or approval should be obtained in all instances where the witness is between the age of 18 and 21 and is still living at his/her parents' or guardian's home; and
- Individuals between 18 and 21, not living with a parent or guardian, may be interviewed without parental approval, except in a morals case, when approval should be obtained. Where parental approval cannot feasibly be obtained, document attempts to obtain approval, and conduct the interview with a witness present.

210.22 Statement Analysis Questionnaire.
The Statement Analysis Questionnaire is an interviewing technique used in situations where there is no definite suspect and any one of a number of people may have committed the offense. The Statement Analysis Questionnaire consists of a specially developed and organized set of questions, either asked orally or in questionnaire form by an SA, which elicits responses indicative of truthfulness or deception on the part of the interviewee. An analysis of the interviewees' responses narrows down the number of suspects, and follow-up interviews are subsequently held with those who may still be suspects.

Only SAs trained in the Statement Analysis Questionnaire technique should administer the questionnaire.

Statement Analysis Questionnaires are treated as subject interviews. Each IRS or TIGTA employee completing the questionnaire should be given Form OI 5230. Bargaining unit employees should also be given IRS Form 8111.

TIGTA procedures regarding the use of warning forms with Statement Analysis Questionnaires have been disseminated to bargaining unit employees and are available on the Internet at www.treas.gov/tigta/oi_interview.shtml, paragraph 16.

210.23 Polygraph Examinations.
The polygraph is a scientific, diagnostic instrument that records physiological changes in a person. It can be reliable in detecting deception by a person on a specific issue. If deception is indicated, the person must be interviewed to obtain the truth.
Be selective when considering the polygraph as an investigative tool; make all other reasonable investigative efforts prior to using the polygraph. Before using the polygraph, consider the following:

- SAs are prohibited from using the polygraph to screen a large number of suspects;
- Use the polygraph in criminal cases, or where extraordinary circumstances merit its use in non-criminal matters;
- Polygraph examination results can be submitted as evidence in an employee investigation for the purpose of administrative adjudication;
- Polygraph examinations are considered subject interviews. Bargaining unit employees should be provided with Form 8111 prior to the examination. TIGTA may determine not to conduct a polygraph examination unless the bargaining unit employee waives the right to union representation; and
- Individuals who submit to a polygraph examination based on allegations against an employee must acknowledge in writing that the polygraph results will not be used against the Government in civil litigation. See Exhibit(400)-210.1.

210.23.1 Polygraph Examination Assistance. Polygraph examinations will generally be conducted by the United States Secret Service (USSS). Exceptions to using the USSS are:

- A joint investigation with another agency which has its own polygraph examiners; and
- Exigent circumstances which may dictate the services of a State or local agency.

210.23.2 Authorization and Approval for Polygraph Examinations. The SAC may authorize polygraph examinations.

SAs cannot initiate any discussion of a polygraph examination, or ask any person to submit to a polygraph examination, without the prior approval of the SAC.

210.23.2.1 Factors for Approval. Consider the following factors when evaluating the use of a polygraph examination:

- Have all reasonable investigative efforts been made?
- Has the person to be examined been interviewed?
- Is the polygraph examination essential for additional information in the investigation?
- Is there reasonable cause to believe that the person to be examined is withholding information relevant to the investigation?
- Is there reasonable cause to believe the person has knowledge of, or is involved in, the matter?
- Does the allegation involve a criminal or non-criminal matter? If non-criminal, are there exceptional circumstances to warrant a polygraph examination?
- Has the person to be examined volunteered for the polygraph examination?
- Will the use of a polygraph examination jeopardize any Federal or local prosecution?

210.23.2.2 Requests for Approval. Prepare a memorandum to the SAC to request a polygraph examination. The memorandum must include the following information:

- The name and age of the person to be examined (if a minor is to be examined, obtain written parental permission and inform the minor's parents that they may be present during the examination);
- Whether the person to be examined is an IRS employee or non-employee (if an IRS employee, include his/her position and grade);
- The case number and case category;
- A brief summary of the facts of the case including the involvement of the person to be examined (list the amount of money involved if monetary theft or bribery occurred);
- Whether the person to be examined requested the polygraph examination, or was asked to submit to a polygraph examination;
- Confirmation that the person to be examined has agreed to the polygraph examination;
- If the person to be examined is a bargaining unit employee, confirmation that the employee waives his/her right to union representation during the examination;
- The city and State where the polygraph examination is to be conducted; and
- The name and telephone number of the case SA.

210.23.3 Requesting USSS Assistance. SAs should fully understand the preceding requirements and procedures prior to initiating any polygraph examination inquiry. Become familiar with USSS policies and procedures before contacting USSS polygraph examiners. See Section 210.22.3.3.

210.23.3.1 Memorandum Requesting Assistance. After approval by the SAC, prepare a memorandum to the Assistant Director of Investigations, USSS, requesting polygraph examination assistance. Include all relevant information.

Submit the memorandum to the local USSS office SAC who will forward the request to USSS headquarters, Forensic Services Division. USSS headquarters will notify the local USSS office SAC of its approval or disapproval of the request. If approved, the polygraph examination will be scheduled through the local USSS office.

210.23.3.2 Polygraph Examiner. Once the polygraph examination has been approved, contact the USSS polygraph examiner to discuss:

- The date and time of the examination;
- The investigation;
- Key factors which need to be resolved;
- Questions to be asked during the polygraph examination; and
- If necessary, return information as permitted under 26 U.S.C. § 6103. See Section 70.3 for more information on disclosure authority.

210.23.3.3 USSS Policy and Procedures. TIGTA has agreed to follow USSS policy in conducting polygraph examinations which includes the following:

- The polygraph examiner has sole discretion to refuse to conduct or to terminate an examination;
- A complete examination consists of a pre-test phase, an in-test phase, and a post-test phase;
- If the person to be examined is a law enforcement officer and the subject of a TIGTA investigation, the examination will be conducted by two polygraph examiners using a "dual examiner polygraph technique;"
- Examinations may be visually monitored via two-way mirrors, video cameras, etc., with the consent of the polygraph examiner;
- All witnesses to a polygraph examination will be identified in the polygraph report.
- An SA will be available to assist the examiner during the examination and should witness the advisement of rights and consent form signature, and obtain a statement or affidavit from the subject if he/she makes any admissions or confessions; and
- SAs will not report preliminary opinions of the polygraph examination. The polygraph examiner is required to send the report to USSS headquarters for quality control review. USSS headquarters will send a formal Polygraph Examination Report directly to the case SA or through the local USSS office.

DATE: July 1, 2020

CHAPTER 400 – INVESTIGATIONS

(400)-220 Subpoenas and Grand Jury Procedures

220.1 Overview.
This Section outlines the policies and procedures for the use of administrative subpoenas, Federal grand juries, and other considerations for compelling the release of certain information or records. This Section also explains the statutory basis for Treasury Inspector General for Tax Administration (TIGTA) Inspector General subpoenas, their scope, enforceability, and application of various laws, including the Right to Financial Privacy Act (RFPA), the Family Educational Right to Privacy Act (FERPA), the Fair Credit Reporting Act (FCRA), and the Electronic Communications Privacy Act (ECPA).

This section includes information related to the following:

220.1.1 Acronyms Table.

220.2 Subpoena Authority.
The Inspector General has authority under Section 6(a)(4) of the Inspector General Act, as amended, “to require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data in any medium (including electronically stored information, as well as any tangible thing) and documentary evidence necessary in the performance of the functions assigned by this Act, which subpoena, in the case of contumacy or refusal to obey, shall be enforceable by order of

any appropriate United States district court, provided that procedures other than subpoenas shall be used by the Inspector General to obtain documents and information from Federal agencies."

The Program Fraud Civil Remedies Act (PFCRA) also provides the Inspector General with subpoena authority as the investigating official under the Act.

220.3 Administrative Subpoena Restrictions. An administrative subpoena request must be relevant to the investigation and related to the functions designated in the Inspector General Act or PFCRA. Inspector General subpoena authority may not be used to obtain records on behalf of another agency, either Federal or State, or for another office within the Department of the Treasury.

The demand contained in the subpoena must be reasonable and should not be unduly burdensome.

Subpoenaed parties cannot be compelled to create a record that does not already exist (*e.g.*, prepare responses to specific questions). Additionally, TIGTA subpoenas are not available to obtain testimonial evidence, with the exception of statements that attest to the authenticity and completeness of documents provided in response to a TIGTA subpoena.

220.3.1 Restrictions on Disclosure. Disclosure of administratively subpoenaed records will not be made except as required by law (*e.g.,* court order, 26 U.S.C. § 6103, or the Privacy Act).

220.4 Use of Subpoenas in Criminal Investigations.
Where documents are required for a criminal investigation and the investigation has been informally or formally discussed with the Department of Justice (DOJ) and/or United States Attorney's Office (USAO), the use of an Inspector General subpoena to obtain the documents should also be discussed. Where documents are required for an audit by the Office of Audit and there is a related ongoing criminal investigation, coordinate the issuance of a subpoena with Office of Investigations (OI), as well as discuss with the DOJ and/or USAO. Avoid the use of a TIGTA subpoena after a grand jury has convened in a particular matter, and make the request only after discussions with TIGTA Counsel and/or DOJ/USAO.

220.5 Subpoena Requests.
The Operations Division process subpoenas via the Inspector General Subpoena Request Assistance Form (RAF) within the Criminal Results Management System (CRIMES). Special agents (SA) will ensure all relevant information is included and any unusual circumstances are fully explained in the "Justification for Issuance" section of TIGTA Form OI S-001, Subpoena Request. Unusual circumstances consist of information that a reviewer, TIGTA Counsel, or the approving official should be aware

of, such as the number of prior subpoenas issued in the investigation, whether the subpoenaed party is represented by counsel or known to have resisted prior subpoenas. The SA will request an IG subpoena using the appropriate forms. All required forms must be uploaded into the IG Subpoena folder within CRIMES prior to the RAF being submitted to the Operations Division. If SAs are submitting multiple IG subpoenas for the same case, each IG Subpoena folder name shall include the name of the subpoenaed party. SAs will submit one RAF per subpoena.

220.5.1 Subpoena Forms. The following TIGTA OI subpoena forms may be used:

Form Number	Title	Form Number	Title
OI S-001	Subpoena Request	OI S-009	Customer's Sworn Statement for Filing a Challenge
OI S-002	Subpoena	OI S-010	Certificate of Service
OI S-003	Return of Service	OI S-011	Cover Letter to Financial Institution
OI S-004	Customer Authorization to Release Financial Records	OI S-012	Certificate of Compliance with the RFPA
OI S-005	Customer Notice	OI S-013	Post-Notice Following Court-Ordered Delay
OI S-006	Statement of Customer Rights (for RFPA)	OI S-014	Certification for Transferring Records Obtained
OI S-007	Instructions for Completing Challenge	OI S-015	Notice of Transfer of Financial Records
OI S-008	Customer's Motion to Challenge	OI S-016	Notice That No Legal Proceedings Are Contemplated

220.5.2 Processing Subpoena Requests. All OI subpoena requests must include TIGTA Forms OI S-001 and S-002. Subpoena requests will be reviewed and approved by the Assistant Special Agent in Charge (ASAC), and the Deputy Special Agent in Charge (DSAC) or the Special Agent in Charge (SAC) before they are forwarded to the Operations Division for processing. If RFPA applies, additional documents will be required. The approving supervisor will document their approvals by annotating their surname in the footer of TIGTA Form OI S-001. Forward the approved request the Operations Division via a CRIMES "IG Subpoena" RAF. In circumstances where a RAF cannot be generated (*e.g.,* leads or intakes), email the prerequisite documents to the Operations Division via *TIGTA Inv Operations for processing.

The Operations Division will conduct an initial review of the request and forward it to TIGTA Counsel. TIGTA Counsel will review the request and the supporting documentation for legal sufficiency. After Counsel has reviewed the request, the subpoena documents will be prepared for the appropriate Assistant Inspector General for Investigations (AIGI) or the Deputy Assistant Inspector General for Investigations (DAIGI) for signature.

220.6 Service of Subpoenas.
Depending on the circumstances and the target of the subpoena, service may be made in person, electronically under specific conditions, via certified or registered mail, or through the subpoenaed party's counsel or registered agent. For service of natural persons, electronic service, such as via e-mail, should be avoided unless the natural person consents to electronic service. When conducting service electronically, provide a justification in the TIGTA Form OI S-001. If agents have questions regarding the best way to serve a subpoena they should consult with the Operations Division.

Service should be made as soon as reasonably possible after the subpoena is issued.

220.6.1 RFPA Requirements. The RFPA may require additional forms and notices to be sent when serving a subpoena on a financial institution for customer financial records. A full explanation of RFPA requirements begins at Section 220.8.

220.6.2 Place of Appearance and Method of Reception. The place of appearance will normally be at the SA's regular post of duty, but it may be at the premises where the records are held, when more reasonable under the particular circumstances. SAs may elect, if appropriate, for the records to be sent to the requesting SA via registered or electronic mail. In those cases, note the subpoena of this action.

220.6.3 Proof of Service. Proof of service is made by the individual serving the subpoena by executing TIGTA Form OI S-003, *Return of Service* certificate and attaching the executed form to the subpoena. The subpoena, with the executed *Return of Service*, shall become a permanent part of the appropriate investigation file. Scan the completed TIGTA Form OI S-003 Return of Service into .pdf file format and forward to the Operations Division via e-mail to *TIGTA Inv Operations within five calendar days after service.

220.7 Production of Records.
Allow reasonable time for the production of records after service of the subpoena – usually 30 days. Factors to consider include the type and volume of records and the possibility of removal or destruction. Consult with the Operations Division regarding instances requiring an unusually short return time (*i.e.*, less than 10 days).

220.7.1 Return Date. The assigned SA may, at his or her discretion, extend the return date for a limited period of time. Record all extensions of time in the case file on TIGTA Form OI 6501, *Chronological Case Worksheet*. Notify the Operations Division of extensions of time that involve special circumstances or extended periods of time.

220.7.2 Reimbursement. Generally, subpoenaed parties are not entitled to reimbursement from TIGTA for the costs of searching, assembling, and copying subpoenaed records. Corporations are required by law to comply with administrative subpoenas, regardless of compensation. Two notable exceptions to this rule are:

- Financial institutions, as defined in the RFPA, may seek reimbursement for the costs of providing customer financial records; and
- Pursuant to 18 U.S.C. § 2706, telecommunication carriers are authorized to charge a reasonable fee to cover the costs of searching for and providing information responsive to a subpoena. Inspector General subpoenas are an exception from this rule, but only to the extent they seek "records or other information maintained by a common carrier that relate to telephone toll records and telephone listings."

SAs may contact financial institutions and telecommunication carriers prior to initiating the subpoena request to ascertain the types of records available and any fees that may apply. This step may help ensure the subpoena seeks necessary information in a cost-effective manner.

Upon receipt of an invoice for records provided by any entity, the recipient will forward the invoice to the Operations Division via e-mail to *TIGTA Inv Operations. The Operations Division will coordinate with TIGTA Counsel to determine if reimbursement is authorized. As appropriate, the division requesting the subpoenaed documents will pay the invoices. If the invoice should not be paid, TIGTA Counsel will assist OI with the preparation of a letter to inform the subpoenaed party that payment is not authorized by law. OI will retain a copy of the letter it sends to the subpoenaed party in the case file.

220.7.3 Noncompliance. If the target of the subpoena does not comply with the subpoena, the assigned SA will advise the ASAC, DSAC/SAC, and the Operations Division promptly and will provide details describing the relevant circumstances. The SAC will ensure coordination with TIGTA Counsel to develop strategy and procedures to ensure compliance. If enforcement action is required, it will be coordinated with DOJ and/or USAO.

220.7.4 Return of Records. Return original documents to their custodian upon completion of all TIGTA interests. Obtain a receipt for all returned documents, originals or copies. A matter is considered complete when the TIGTA investigation is terminated

and no further use is required of the subpoenaed material in any civil, criminal, or administrative proceeding.

220.8 Applicability of the Right to Financial Privacy Act.
The Right to Financial Privacy Act (RFPA) imposes additional requirements and restrictions on the use of administrative subpoenas to obtain customer financial records from a “financial institution" as defined in the RFPA. The primary requirement involves prior notification to an individual or non-corporate customer and an opportunity for the customer to challenge the subpoena in U.S. District Court.

The following records are not subject to the provisions of the RFPA:
- Financial records of a corporation; and
- Financial records of partnerships of more than five individuals.

The Operations Division may be consulted if there are any questions regarding RFPA subpoenas.

220.8.1 Definitions. The RFPA applies solely to financial records held by a financial institution. Definitions are set forth in 12 U.S.C. § 3401 of the RFPA. The following definitions apply to the RFPA:

- **Person –** is an individual or partnership of five or fewer individuals. The RFPA does not apply to bank records of corporations, trusts, associations, or larger partnerships. It also does not apply to deceased account holders.
- **Customer –** is any person or authorized representative of that person who is using or has used any service of a financial institution, or for whom a financial institution is acting or has acted as a fiduciary to an account maintained in the person's name.
- **Financial institution –** is any office of a bank, savings bank, credit card issuer, industrial loan company, trust company, savings association, building and loan, or homestead association including cooperative banks, credit union, or consumer finance institution located in any State or territory of the U.S., the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands.
- **Financial record –** is an original of, copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer’s relationship with the financial institution. The account must be in the customer’s true name. Accordingly, the RFPA does not apply to forged or counterfeit financial instruments or records concerning an account maintained under a fictitious name.
- **Law enforcement inquiry –** means a lawful investigation of a violation of any criminal or civil statute, regulation, rule or order.

220.8.2 Subpoena Requests Under RFPA. In addition to TIGTA Forms OI S-001 through S-003, which are utilized for any IG subpoena, TIGTA Forms OI S-004 through S-016 are utilized to comply with the provisions of the RFPA.

The following chart summarizes the TIGTA Forms, which shall be prepared for the various parties.

The following forms shall be prepared for the customer:	
OI S-002	Subpoena (copy)
OI S-004	Customer Authorization to Release Financial Records
OI S-005	Customer Notice
OI S-006	Statement of Customer Rights (for RFPA)
OI S-007	Instructions for Completing Challenge
OI S-008	Customer's Motion to Challenge
OI S-009	Customer's Sworn Statement for Filing a Challenge
OI S-010	Certificate of Service
The following forms shall be prepared for the financial institution:	
OI S-002	Subpoena (original)
OI S-011	Cover Letter to Financial Institution
OI S-012	Certificate of Compliance with the RFPA

The original subpoena (S-002) is served on the financial institution along with the Cover Letter to the Financial Institution (S-011).

A copy of the subpoena (S-002), the Customer Authorization to Release Financial Records (S-004), the Customer Notice (S-005), the Statement of Customer Rights (S-006), the Instructions for Completing Challenge (S-007), the Customer's Motion to Challenge (S-008), the Customer's Sworn Statement for Filing a Challenge (S-009), and the Certificate of Service (S-010) are concurrently served on the customer whose financial records are sought by the subpoena.

If no customer challenge has been filed, the case agent will notify the Operations Division when 10 days have elapsed from the date of personal service of the subpoena, customer notice and related forms to the customer or when 14 days have elapsed from the date of mailing the subpoena, customer notice and related forms to the customer that no customer challenge has been filed. The case agent will complete the required information in the Certificate of Compliance (S-012) and forward the form to the Operations Division who will obtain the signature of the appropriate DAIGI/AIGI. The Operations Division will provide the financial institution with the Certificate of Compliance (S-012). The appropriate DAIGI/AIGI will sign the Certificate of Compliance.

220.9 Basic Requirements of the RFPA.
The RFPA imposes certain basic requirements regarding:

- Restrictions on Government access;
- Notice to customer;
- Delayed notice;
- Government certification of compliance with the RFPA;
- Challenge; and
- Use of information.

220.9.1 Restrictions on Government Access. The RFPA prohibits any government authority, Federal department or agency from accessing or obtaining from a financial institution copies of, or accessing or obtaining the information contained in, the financial records of any customer unless the financial records are reasonably described and either:

- The customer has authorized disclosure;
- Disclosure is authorized by an administrative subpoena or summons;
- Search warrant;
- Judicial subpoena; or
- A formal written request.

The RFPA prohibits a financial institution from releasing to a Federal department or agency any records or information concerning a customer's transactions unless one of the below methods are used.

220.9.1.1 Voluntary Customer Authorization. A customer may authorize access to his/her financial records by signing and dating TIGTA Form OI S-004, Customer Authorization to Release Financial Records. The authorization will identify the records disclosed, the government authority, and purpose for disclosure. The authorization is valid for three months following the date it is signed. The authorization shall include the customer's rights under the RFPA. The customer may revoke the authorization at any time prior to disclosure. If the customer is a bargaining unit employee, consult with the Operations Division prior to requesting voluntary authorization if the request is not made in the course of a subject interview. A properly secured customer authorization nullifies the need for TIGTA Forms OI S-005 through OI S-010.

220.9.1.2 Administrative Subpoena or Summons. An authorized official may issue an administrative subpoena for a customer's financial records if the Government agency has reason to believe that the records sought are relevant to the performance of its mission (*e.g.*, a legitimate law enforcement inquiry). A copy of the subpoena together with TIGTA Forms OI S-004 through S-010 shall be served on the customer or mailed to his/her last known address on or before the date the financial institution is served. TIGTA may obtain the records if 10 days have expired from the date of service of the

notice, or 14 days have expired from the date of mailing the notice, and the customer has not filed a sworn statement or a motion to quash.

220.9.1.3 Search Warrant. When a Government agency obtains access to financial records pursuant to a search warrant, a copy of the search warrant must be mailed to the customer's last known address, together with a notice, no later than 90 days after the search warrant was served. A U.S. District Court may grant a delay in mailing the notice. Upon expiration of delay of notification, a copy of the search warrant must be mailed to the customer along with the notice.

220.9.1.4 Judicial Subpoena. A copy of the subpoena shall be served on the customer or mailed to his/her last known address on or before the date the financial institution is served. This mail will also include a notice to the customer, motion paper, and sworn statement. Grand jury subpoenas are exempt from this requirement.

Records shall not be released until the Government certifies in writing to the financial institution that it has complied with the RFPA. A financial institution which makes a disclosure in good faith reliance upon a certificate is relieved of any liability to the customer in connection with the disclosure. See TIGTA Form OI S-012.

The RFPA requires that a customer is given prior notice when the Government attempts to gain access to information concerning his/her financial transactions. Include the location of appropriate Federal district courts in the Customer Notice, including the U.S. District Court for the District of Columbia, the district court which has jurisdiction over the customer's last known address, and the district court which has jurisdiction over the address of the financial institution from which the records are being sought. See TIGTA Forms OI S-005 and S-006.

220.9.1.5 Formal Written Request. SAs are not authorized to use a formal written request to obtain financial records under 31 CFR § 14.3, because TIGTA has administrative subpoena authority pursuant to the Inspector General Act, as amended.

220.9.2 Notice to Customer. The RFPA requires that a customer of a financial institution receives prior notice of the attempt of a government authority to gain access to records or record information held by the financial institution concerning such customer. See TIGTA Form OI S-005, *Customer Notice Form*, for the notice required to be given with a judicial subpoena, administrative subpoena, or formal written request. The notice to the customer is accompanied by a motion paper and sworn statement, which the customer may use to try to quash the subpoena. See TIGTA Form OI S-008, *Customer's Motion to Challenge Government Access to Financial Records Form* and TIGTA Form OI S-009, *Customer's Sworn Statement for Filing a Challenge* Form for samples of each. Customers do not have to use these forms.

220.9.3 Delayed Notice. The government authority may apply to an appropriate court to delay the required notice to the customer for as much as 90 days and to issue an order prohibiting the financial institution from disclosing that records have been obtained or that a request for records has been made. Such delay may be granted if the court finds that notice to the customer will result in endangering the physical safety of any person, or cause flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, or seriously jeopardizing an investigation or official proceeding. Additional extensions of 90 days may be granted by the court upon application. Upon expiration of the delay of notification, the customer shall be served with a copy of the process or request together with TIGTA Form OI S-013, *Post-Notice Following Court-Ordered Delay Form*.

220.9.4 Government Certification of Compliance with RFPA. A financial institution will not release financial records of a customer until the government authority seeking such records certifies in writing that it has complied with all applicable provisions of the RFPA. Such certification relieves the financial institution of any liability to the customer in connection with the disclosure of the financial records.

The SA should serve the subpoena following the instructions outlined in Section 220.9.2. After sufficient time has passed (10 days from the date of service of the customer notice or 14 days from the date of mailing of the customer notice) and the customer has not challenged the subpoena, the SA will complete TIGTA Form OI S-012, *Certificate of Compliance with the Right to Financial Privacy Act*, and forward the TIGTA Form OI S-012, along with a copy of the completed Return of Service, to the Operations Division via e-mail to *TIGTA Inv Operations, to obtain the appropriate DAIGI/AIGI signature. The Operations Division will mail the signed TIGTA Form OI S-012 to the financial institution.

See TIGTA Form OI S-012, *Certificate of Compliance with the Right to Financial Privacy Act*, for sample certification format.

220.9.4 Challenge. In general, the RFPA provides that the individual whose financial records are being sought may challenge the Government's access to his/her records by filing a motion in Federal district court to quash the administrative subpoena or an application to enjoin the Government authority from obtaining financial records. Such filings must take place within 10 days of service or 14 days of mailing of the customer notice. The notice to the customer is accompanied by a motion and sworn statement, which the customer may use to challenge the subpoena in U.S. district court. See TIGTA Forms OI S-007 through S-010.

220.9.4.1 Motions to Quash and Applications to Enjoin. The RFPA provides that the customer of a financial institution may challenge the Government's access to his or her records if, within 10 days of service or 14 days of mailing a subpoena or formal written request, the customer files in the appropriate Federal court a motion to quash the

administrative subpoena or judicial subpoena or an application to enjoin a Government authority from obtaining access pursuant to a formal written request. If the customer files a motion to quash and, in the opinion of the court, complies with the RFPA's procedural requirements, the court will order the government to file a sworn response.

220.9.4.2 Appeals. A court ruling denying a customer's motion to quash is not a final order and an interlocutory appeal may not be taken by the customer. If no legal proceeding is to be commenced against the customer, an appeal may be made within 30 days of a notification to that effect.

The USAO can appeal an adverse final judgment. The customer must be notified within 30 days of the USAO's decision to appeal an adverse ruling. An appeal may be taken within 30 days of such notification. In the event that no determination regarding a legal proceeding is made within 180 days, a certification may be required by the court until the investigation is concluded.

220.9.5 Use of Information. Unless certain exemptions apply, financial records that OI SAs originally obtain pursuant to the RFPA shall not be transferred to any other agency or department, including DOJ, unless TIGTA certifies in writing that there is reason to believe that the records are relevant to a legitimate law enforcement inquiry within the jurisdiction of the receiving agency or department. After consulting with TIGTA Counsel, the appropriate DAIGI/AIGI shall sign the appropriate certification. In addition, within 14 days of the transfer, the ASAC shall send a copy of the certification to the customer notifying him/her of the nature of the law enforcement inquiry and his/her rights pursuant to the RFPA. Court orders may be used to delay this notice. See TIGTA Form OI S-014, *Certification for Transferring Records Obtained Pursuant to the Right to Financial Privacy Act of 1978 Form* and TIGTA Form OI S-015, *Notice of Transfer of Financial Records Form*. The SA will record the disclosure on TIGTA Form OI 6501.

However, records may be transferred to DOJ and the Department of the Treasury upon the certification by a supervisory TIGTA official that there is reason to believe that the records may be relevant to a violation of Federal criminal law; and the records were obtained in the exercise of TIGTA's supervisory or regulatory functions.

220.10 Exceptions to the RFPA.
Exceptions or special procedures to the RFPA are provided in 12 U.S.C § 3413.

220.11 Emergency Access to Financial Records.
When there is reason to believe that delay in obtaining financial records from a financial institution would create imminent danger of physical injury to any person, serious property damage, or flight to avoid prosecution, submit to the financial institution the certification of compliance with the RFPA. See TIGTA Form OI S-012. In addition:

- Within five days of access, a sworn statement setting forth the grounds for emergency access by the above TIGTA official must be filed with the appropriate court.
- As soon as possible after the records have been obtained, unless a court issued delay order is instituted, mail or serve a copy of the request together with notification of emergency access to the customer. See Exhibit (400)-60.1 for sample format.

220.12 Applicability of the Family Educational Right to Privacy Act.
The Family Educational Right to Privacy Act (FERPA), 20 U.S.C. § 1232g, imposes additional restrictions on the use of administrative subpoenas to obtain educational records from an educational agency or institution.

220.12.1 Definitions. The FERPA applies solely to educational records held by an educational agency or institution as defined in § 1232g(a) of the FERPA.

Educational records - are defined as those records, files, documents, and other materials that contain information directly related to a student and that are maintained by an educational agency or institution. For the most part, "educational records" maintained by the educational institution are available for student review.

Educational agency or institution – is defined as any public or private agency or institution that is the recipient of funds under any applicable program.

FERPA does not apply to other types of records maintained by an educational institution, such as (1) personal notes or records (including computerized files) that are kept by an employee of the educational institution maintained solely in her or his possession, (2) records that relate to an employee (except student employees), (3) medical and psychiatric records created, maintained, and used only in connection with the treatment of a student and that are not available to anyone other than the persons providing such treatment, or (4) records that contain information relating to a person only after that person is no longer a student (*i.e.*, alumni records).

220.12.2 Student Notification Requirement. Prior to disclosing a student's educational records in response to a subpoena, the educational institution must make a reasonable effort to notify the student of the subpoena in advance of compliance, so that the student may seek protective action, unless the subpoena is issued for a law enforcement purpose and the issuing agency has ordered that the existence or the contents of the subpoena not be disclosed. See 34 C.F.R. § 99.31(9).

220.12.3 Subpoena Requests Under FERPA. SAs requiring educational records under FERPA will detail the need for such records on TIGTA Form OI S-001 and clearly state whether the SA recommends that TIGTA order that the educational institution not

disclose the existence of the subpoena (or the information furnished in response to the subpoena) to the student.

220.13 Applicability of the Electronic Communications Privacy Act of 1986.
The Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–2522, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. ECPA includes the Pen Register Statute and the Stored Communications Act (SCA), as well as amendments to the Wiretap Act. These statutes are part of a set of laws that control the collection and disclosure of both content and non-content information related to electronic communications, as well as content that has been stored remotely. Although originally enacted in 1986, since then, ECPA has been updated several times. As the law is constantly evolving, SAs should contact TIGTA's Office of Chief Counsel and/or their relevant USAO if they have specific legal questions.

220.14.4 Compelled Disclosure. There are five mechanisms that a government entity can employ to compel a provider to disclose the contents of stored wire or electronic communications (including e-mail and voice mail) and other information such as account records and basic subscriber and session information. The five mechanisms are:

- Subpoena;
- Subpoena with prior notice to the subscriber or customer;
- § 2703(d) court order;
- § 2703(d) court order with prior notice to the subscriber or customer; and
- Search warrant.

220.14.4.1 Subpoena. The SCA permits the government to compel disclosure of the basic subscriber and session information as listed in 18 U.S.C. § 2703(c)(2) from "service providers" using a subpoena. What constitutes a service provider as applicable to a subpoena is evolving but it generally involves electronic communications and computer processing. For example, it is likely that Apple in relation to iCloud is a service provider but Apple in relation to brick and mortar Apple Stores would likely not be considered a service provider. See TIGTA's Subpoena Guide for the most current language and examples.

220.14.4.2 Subpoena with Prior Notice to the Subscriber or Customer. Agents who obtain a subpoena and either give prior notice to the subscriber or comply with the delayed notice provisions of § 2705(a) may obtain:

- Everything that can be obtained using a subpoena without notice;
- "The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than 180 days;" [See 18 U.S.C. § 2703(a)]

- "The contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of... a subscriber or customer of such remote computing service." [See 18 U.S.C. §§ 2703(b)(1)(B)(i) and 2703(b)(2)].

220.14.4.2.1 Notice Provisions. The notice provisions can be satisfied by giving the customer or subscriber "prior notice" of the disclosure. See 18 U.S.C. § 2703(b)(1)(B). However, 18 U.S.C. § 2705(a)(1)(B) permits notice to be delayed for 90 days "upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result." See 18 U.S.C. § 2705(a)(1)(B). Both "supervisory official" and "adverse result" are specifically defined terms for the purpose of delaying notice. See 18 U.S.C. § 2705(a)(2) (defining "adverse result") and 18 U.S.C. § 2705(a)(6) (defining "supervisory official"). This provision of the SCA provides a permissible way for the government to delay notice to the customer or subscriber when notice would jeopardize a pending investigation or endanger the life or physical safety of an individual. The Government may extend the delay of notice for additional 90-day periods through additional certifications that meet the "adverse result" standard of § 2705(b). See 18 U.S.C. § 2705(a)(4). Upon expiration of the delayed notice period, the statute requires the government to send a copy of the request or process along with a letter explaining the delayed notice to the customer or subscriber. See 18 U.S.C. § 2705(a)(5).

220.14.4.3 Section 2703(d) Order. A § 2703(d) court order is required to obtain most account logs and most transactional records. With a § 2703(d) court order you may obtain:

- Anything that can be obtained using a subpoena without notice; and
- All "record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])." See 18 U.S.C. § 2703(c)(1).

A court order authorized by 18 U.S.C. § 2703(d) may be issued by any Federal magistrate, district court, or equivalent state court judge. See 18 U.S.C. §§ 2703(d), 2711(3). To obtain such an order, the governmental entity must offer specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. See 18 U.S.C. § 2703(d).

220.14.4.4 2703(d) Order with Prior Notice to the Subscriber or Customer. Investigators can obtain everything associated with an account except for unopened e-mail or voicemail stored with a provider for 180 days or less using a 2703(d) court order that complies with the notice provisions of § 2705. Investigators who obtain a court order under 18 U.S.C. § 2703(d), and either give prior notice to the subscriber or else comply with the delayed notice provisions of § 2705(a), may obtain:

- Everything that can be obtained using a § 2703(d) court order without notice;
- "The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than 180 days," See 18 U.S.C. § 2703(a).
- "The contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." See 18 U.S.C. § 2703(b)(1)(B)(ii) and 18 U.S.C. § 2703(b)(2).

220.14.4.4.1 Notice Provisions. As an alternative to giving prior notice, law enforcement can obtain an order delaying notice for up to 90 days when notice would seriously jeopardize the investigation. The legal standards for obtaining a court order delaying notice mirror the standards for certified delayed notice by a supervisory official. See 18 U.S.C. § 2705(a). The applicant must satisfy the court that there is reason to believe that notification of the existence of the court order may: endanger the life or physical safety of an individual; lead to flight from prosecution; lead to destruction of or tampering with evidence; lead to intimidation of potential witnesses; or... otherwise seriously jeopardize an investigation or unduly delay a trial." See 18 U.S.C. §§ 2705(a)(1)(A) and 2705(a)(2). The applicant must satisfy this standard anew in every application for an extension of the delayed notice.

220.14.4.5 Search Warrant. Investigators can obtain everything associated with an account with a search warrant. The SCA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant. Agents who obtain a search warrant under § 2703 may obtain:

- Everything that can be obtained using a § 2703(d) court order with notice; and
- "The contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for 180 days or less." See 18 U.S.C. § 2703(a).

220.15 Applicability of the Fair Credit Reporting Act.
The Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681, FCRA limits consumer credit reporting agencies from furnishing consumer reports, also known as credit reports, except under specified circumstances. Some of the specified circumstances follow:

- A consumer reporting agency may furnish a credit report to a Government agency if the information is for employment purposes, and the Government agency has written authorization from the consumer.
- A consumer reporting agency may furnish to a Government agency identifying information regarding any consumer, limited to the consumer's name, address, former address, places of employment, and former places of employment.

220.15.1 Credit Report Use in Investigations. The FCRA restricts law enforcement agencies' use of credit reports. TIGTA may access credit reports on the subject of an investigation only under the following circumstances:

- The individual furnishes written consent; or
- By grand jury subpoena.

220.15.2 Requesting Credit Reports. All requests for credit reports (except through a Federal grand jury subpoena or other court order) will be made by submitting an RAF via CRIMES to the Fraud and Schemes Division (FSD).

The request must include the name, address, Social Security Number, and date of birth of the subject of the credit report, along with the case number and the requestor's name and fax number. The request must also be accompanied by a properly prepared TIGTA Form OI 2760, *Authorization for Release of Credit Reports*, signed by the subject of the credit report.

FSD will forward the resulting credit reports to the requesting agent as soon as they are available.

When considering a request for credit reports in conjunction with any investigation, remember that the consumer reporting agency may notify the consumer involved that a report has been furnished to or requested by TIGTA.

220.16 Grand Jury Subpoenas.
Grand jury subpoenas are governed by Rule 17 of the Federal Rules of Criminal Procedure (FRCP). Federal grand jury subpoenas may be served at any place within the United States and enforceable in Federal court.

Grand jury subpoenas can be issued to compel a) testimony (*ad testificandum*); b) the production of documents or objects (*duces tecum*); or c) both.

220.16.1 Access to Grand Jury Information. Rule 6(e) of the FRCP governs the secrecy and permissible disclosure of grand jury information. Rule 6(e) permits disclosure of matters occurring before the grand jury to such TIGTA personnel as are deemed necessary by an attorney for the Government to assist in the performance of such attorney's duty to enforce Federal criminal law.

SAs will ensure grand jury information, to include a separate Form OI 6501, regarding grand jury related activity, is stored in an access-restricted folder within CRIMES. SAs will only allow authorized individuals access to the restricted folder. See the CRIMES Help Guide Library for additional information.

Do not disclose matters occurring before the grand jury to anyone, including other TIGTA personnel, except as deemed necessary by the attorney for the Government. Matters occurring before the grand jury include all documents and testimony obtained by grand jury subpoena.

220.16.2 Special Agent Assisting the Attorney for the Government in a Grand Jury Matter. Grand jury matters may be disclosed to any Government personnel that an attorney for the Government considers necessary to assist in performing that attorney's duty to enforce Federal criminal law. If a TIGTA SA is assisting the Government's attorney under Rule 6(e), the SA shall immediately give the Government attorney the names of relevant OI personnel to be included on the grand jury disclosure list, or "6(e)" list. The list shall include all personnel necessary to manage the grand jury material and oversee the SA's job performance. The list may contain leadership and appropriate support personnel.

220.16.3 Disclosure of Grand Jury Material in Judicial Matters. Grand jury matters may not be disclosed except as permitted by Rule 6(e) of the FRCP.

TIGTA may use grand jury information for non-criminal law enforcement purposes only upon the issuance of a court order under Rule 6(e) directing disclosure of matters occurring before the grand jury for the purpose of civil liabilities.

See Section 250.17 for information regarding the protection of grand jury information and grand jury case closing procedures.

CHAPTER 400 – INVESTIGATIONS

(400)-230 Victim/Witness Program

230.1 Overview.
This section provides guidance on the Office of Investigations (OI) Victim/Witness Program. This policy applies to all Treasury Inspector General for Tax Administration (TIGTA) Special Agents (SA) and to other OI employees whose duties may impact victims/witnesses encountered during the course of OI investigations. OI's policy is intended to apply in all cases specified by the victim and witness laws when permissible under 26 U.S.C. § 6103. This section includes information related to the following areas:

- Authority and Title 26 Interaction
- Agency Victim/Witness Coordinator
- Statutes for Victim Services and Rights
- Victim
- Victim and Witness Assistance
- Child Victims
- Other Vulnerable Victims
- Victims of Identity Theft
- Foreign Victims
- Temporary Protective Measures
- Witness Security Reform Act of 1984

230.1.1 Acronyms Table.

230.2 Authority and Title 26 Interaction.
The Victim and Witness Protection Act of 1982 (VWPA) instructed the Attorney General to ensure that all Federal law enforcement agencies adopt guidelines consistent with the purposes of the VWPA. The Victim/Witness Program, as described in this section, conforms to the 2011 Attorney General Guidelines for Victim and Witness Assistance (2011 AG Guidelines – Rev. May 2012). Where TD 55-01 conflicts with the 2011 AG Guidelines - Rev. May 2012, this policy adopts the 2011 AG Guidelines - Rev. May 2012.

When enforcement of the victim/witness laws conflicts with the requirements of 26 U.S.C § 6103, compliance with 26 U.S.C § 6103 generally takes precedence over compliance with the victim and witness laws. Contact the National Victim/Witness Coordinator (NVWC), through your Divisional Victim/Witness Coordinator (DVWC), who shall consult with TIGTA Counsel for guidance in these situations.

230.3 Agency Victim/Witness Coordinator.
OI has a National Victim/Witness Coordinator assigned to Headquarters Operations Division, and each Division has a designated DVWC.

230.3.1 National Victim/Witness Coordinator. The NVWC is assigned to the Assistant Special Agent in Charge (ASAC)-Policy Team and is responsible for:

- Maintaining OI's policy;
- Facilitating communication among OI employees, OI management, TIGTA Counsel, the U.S. Department of Justice (DOJ), and other outside agencies;
- Ensuring victim/witness policy changes are reviewed with DVWCs within a reasonable time period after any changes in the AG Guidelines or victims' rights laws take effect; and
- Providing guidance to OI employees, as necessary, regarding the requirements of Federal victim and witness laws.

230.3.2 Divisional Victim/Witness Coordinator. The DVWC is responsible for:

- Ensuring that newly hired SAs are provided an overview of OI's victim/witness policy, to include the identification of abused children and the SA's obligation to report suspected child abuse. See Section 230.7.1 for information on reporting suspected child abuse;
- Ensuring victim/witness policy changes are reviewed with SAs within a reasonable time period after any changes in the AG Guidelines or victims' rights laws take effect;
- Assisting SAs and division management in the accomplishment of local responsibilities under this policy;
- Maintaining contact information for the U.S. Attorney's Office (USAO) Victim/Witness Coordinator in the division's geographical area. USAO resources can be found via the U.S. Department of Justice website; and
- Maintaining a telephone and address listing of Victim/Witness service providers located in the division's geographical area. Resource information is available via the U.S. Department of Justice, Office for Victims of Crime's website.

230.4 Statutes for Victim Services and Rights.
There are two core statutes applied to Federal crime victim programs:

- The Victims' Rights and Restitution Act (VRRA), 34 U.S.C. § 20141 (1990). This statute is most relevant for use during the investigative stage and attaches at identification of the victim.

- The Crime Victims' Rights Act (CVRA), 18 U.S.C. § 3771 (2006 & Supp. III 2009). The victim rights under this statute attach upon the filing of charges and are typically administered by the USAO Victim/Witness Coordinator.

The VRRA (34 U.S.C. § 20141) provisions are generally referred to as "services" and are distinguished from victims' "rights," which are contained in the CVRA (18 U.S.C. § 3771).

230.5 Victim.
A victim of a crime is defined as follows:

- Per the VRRA, a person that has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime, including the situations below. 34 U.S.C. § 20141(e)(2).

    - In the case of an institutional entity, an authorized representative of the entity; and,
    - In the case of a victim who is under 18 years of age, incompetent, incapacitated, or deceased, one of the following (in order of preference):

        - A spouse;
        - A legal guardian;
        - A parent;
        - A child;
        - A sibling;
        - Another family member; or
        - Another person designated by the court.

Per the CVRA, a person directly and proximately harmed as a result of the commission of a Federal offense or an offense in the District of Columbia. 18 U.S.C. § 3771(e).

Note: Each of the statutes has a slightly different definition of a crime victim. Accordingly, there may be some victims who qualify to receive services under the VRRA, but who will not be able to enforce crime victims' rights under the CVRA.

230.5.1 Victims Under the OI Victim/Witness Program. Usually only those persons suffering direct physical, emotional, or pecuniary harm are considered victims for purposes of the OI Victim/Witness Program. Thus, persons whose injuries are indirectly caused by the crime are not typically entitled to services. While bystanders are generally not considered victims, there may be circumstances when a bystander does suffer direct injury, and OI employees may provide such persons with appropriate assistance within available resources.

In cases involving tax administration or other financial crimes in which a person not charged with an offense suffers harm due to his/her own willful participation in a scheme (*i.e.*, a participant in a refund scheme), a determination of direct harm is generally negated. See the 2011 AG Guidelines – Rev. May 2012, Article III, Commentary.

230.6 Victim and Witness Assistance.
OI is committed to providing crime victims and witnesses the rights and services required by Federal law. OI employees are expected to exercise sound judgment and discretion in deciding how best to afford victims and witnesses the rights and services required under Federal law, as described in this policy. When not prohibited by another statute, there is a presumption in favor of providing, rather than withholding, assistance and services to victims and witnesses of crime. See Section 230.9 for information related to victims of identity theft. See Section 230.7 for information related to child victims.

230.6.1 Responsibilities for Providing Services to Crime Victims. OI's responsibilities begin when an investigation within TIGTA's jurisdiction begins, and extends through the prosecution of the case. Once an investigation has transferred to the prosecutorial entity or charges are filed, officials from the prosecutorial entity are responsible for informing and assisting victims. However, if a victim has already received referrals for services from the investigative agency, the prosecutorial and investigative agencies should attempt to coordinate their efforts to ensure consistency and meet the best interests of the victim. See 2011 AG Guidelines - Rev. May 2012, Article IV, G, H, and I.

At the earliest opportunity after detection of a crime at which it may be done without interfering with an investigation, the responsible SA or other OI employee shall:

- Identify the victim(s) of the crime;
- Provide victims/witnesses with information regarding the services and rights available to them under law, as applicable and when permissible under 26 U.S.C. § 6103 (See Section 230.6.2);
- Keep Division management apprised of any issues that may require additional resources or management guidance;
- Inform the victim(s) of the name, title, business address, and telephone number of the responsible DVWC to whom a request for services should be addressed as appropriate; and
- Provide reasonable assistance in contacting appropriate offices or coordinators providing suitable services.

See 34 U.S.C. § 20141(b).

The Special Agent in Charge (SAC) and ASAC are responsible for:

- Providing SAs with sufficient guidance and resources to meet the requirements of this policy; and
- Coordinating with OI Headquarters, DOJ, and outside organizations as necessary to implement the requirements of this policy.

SAs should immediately notify their ASAC, who will in turn notify the SAC, concerning actual instances of intimidation or harassment of any victim or witness, and/or when a victim or witness requires protection against threats, harm, or intimidation.

Complaint Management Team (CMT) employees who receive complaints shall notify their first-line supervisor immediately upon determining a situation exists in which the provisions of victim/witness laws could be invoked. CMT's supervisor will refer matters involving a specific Division to the respective DVWC and all other matters to the NVWC.

230.6.2 Victim Notification. At the earliest opportunity after the initiation of an investigation, subject to the provisions of 26 U.S.C. § 6103, the SA should provide victims/witnesses with information regarding the services (See Section 230.6.3) and rights (See Section 230.6.4) available to them under law. Unless the prosecuting agency has assumed responsibility for providing such information.

To comply with the requirements regarding victims' rights and the services to which they may be entitled, SAs shall provide a TIGTA OI Victim/Witness Brochure to victims and witnesses as soon as they are identified, unless such notification would violate the confidentiality requirements of 26 U.S.C. § 6103 or jeopardize the investigation. Questions regarding assistance and services to victims and witnesses should be referred to the DVWC, who will contact the NVWC, as necessary.

Note: The nature and extent of services provided may vary with the type of harm experienced by the victim and other surrounding circumstances.

230.6.3 Victim Services. Victim services might include the following:

- Informing the victim of his/her rights as described in 230.6.4 of this Section;
- Informing the victim of the place where the victim may receive emergency medical or social services. 34 U.S.C. § 20141(c)(1)(A);
- Informing the victim of the availability of any restitution or other relief (including crime victim compensation programs for victims of violent crimes) to which the victim may be entitled under this or any other applicable law, and the manner in which such relief may be obtained. 34 U.S.C. § 20141(c)(1)(B) and 18 U.S.C. § 3664;
- Informing the victim of public and private programs that are available to provide counseling, treatment, and other support to the victim. 34 U.S.C. § 20141(c)(1)(C);

- Informing the victim of the availability of payment for testing and counseling in cases of sexual assaults. 34 U.S.C. § 20141(c)(7);
- Informing the victim of the availability of services for victims of domestic violence, sexual assault, or stalking. Reference the 2011 AG Guidelines - Rev. May 2012, Article III, L, 2 for additional guidance in dealing with these victims;
- Providing the victim with the status of the investigation of the crime, to the extent it is appropriate and will not interfere with the investigation. 34 U.S.C. § 20141(c)(3)(A);
- Notifying the victim of the arrest of a suspected offender. 34 U.S.C. § 20141(c)(3)(B);
- Notifying the victim of the availability of protection from a suspected offender and persons acting in concert with, or at the behest of, the suspected offender. 34 U.S.C. § 20141(c)(2);
- Providing the victim with the assurance that any property of the victim that is being held as evidence is maintained in good condition and will be returned to the victim as soon as it is no longer needed for evidentiary purposes. 34 U.S.C. § 20141(c)(6);
- Providing assistance (upon request of the victim or witness) to the victim with notifying the employer of the victim or witness if cooperation in the investigation of the crime causes his/her absence from work; and/or the creditors of a victim or witness, when appropriate, if the crime or cooperation in the investigation affects his/her ability to make timely payments. 2011 AG Guidelines - Rev. May 2012, Article IV, L; and
- Providing assistance to the victim with respect to transportation, parking, childcare, translator services, and other investigation-related services. Upon filing of charges by the prosecutor, this responsibility transfers to the responsible official of the prosecutorial agency. 2011 AG Guidelines - Rev. May 2012, Article IV. G, 2.

230.6.4 Victim Rights. 18 U.S.C. § 3771(c) provides that "officers and employees of the Department of Justice and other departments and agencies of the United States engaged in the detection, investigation, or prosecution of crime shall make their best efforts to see that crime victims are notified of, and accorded, the following rights:

- The right to be reasonably protected from the accused;
- The right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused;
- The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding;

- The right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding;
- The reasonable right to confer with the attorney for the Government in the case;
- The right to full and timely restitution as provided by law;
- The right to proceedings free from unreasonable delay; and
- The right to be treated with fairness and with respect for the victim's dignity and privacy."

See 18 U.S.C. § 3771(a) for the rights of crime victims.

In the case of a victim who is under 18 years of age, incompetent, incapacitated, or deceased, the legal guardian of the victim or representative of the victim's estate, another family member, or any other person appointed as suitable by the court, may assume the victims' rights, but in no event shall the defendant be named as such representative or guardian. 18 U.S.C. § 3663(a)(2).

230.7 Child Victims.
In addition to the victims' rights listed in Section 230.6.4, child victims and witnesses (under age 18) have additional rights in court and throughout the criminal justice system. See 18 U.S.C. § 3509 and the 2011 AG Guidelines - Rev. May 2012, Article III, L,1 for guidelines and appropriate treatment of child victims and witnesses.

230.7.1 Reporting Suspected Child Abuse. Federal law requires all law enforcement personnel working on Federal land or in a Federally operated or contracted facility, in which children are cared for or reside, to report suspected child abuse to the local law enforcement agency or local child protective services agency that has jurisdiction to investigate reports of child abuse or to protect child abuse victims in the area or facility in question. If no local agency is available to assist, the Federal Bureau of Investigation (FBI) shall receive and investigate such reports. See 42 U.S.C. § 13031. If the suspected child abuse is not on Federal land or in a Federally operated or contracted facility, contact the TIGTA Office of Chief Counsel for guidance.

In order to provide immediate notice of suspected child abuse, verbal reports are preferred. However, allegations should be subsequently documented as in any other investigative situation. Reports may be made anonymously. Reports are presumed to have been made in good faith and reporters are immune from civil and criminal liability arising from the report unless they act in bad faith. See 42 U.S.C. § 13031 and the 2011 AG Guidelines - Rev. May 2012, Article III, L,1.

230.8 Other Vulnerable Victims.
Victims of domestic violence, sexual assault, or stalking are particularly vulnerable. Agency personnel should make their best effort to respect the privacy and dignity of these victims, and make victim safety a high priority, as they are often in danger of

future violence after reporting a crime. If neglect, abuse, or exploitation of vulnerable adult victims, such as the elderly or persons with physical or mental disabilities, is suspected, TIGTA Office of Chief Counsel guidance should be sought about potentially contacting Adult Protective Services or local law enforcement. In situations where imminent threat of death or serious bodily injury exists, contact Adult Protective Services or local law enforcement immediately, and notify TIGTA Office of Chief Counsel as soon as practical.

Referrals to the local social services agency best able to meet the needs of the victim should be provided. See 2011 AG Guidelines – Rev. May 2012, Article III, L, 2 and 3 for more information.

230.9 Victims of Identity Theft.
In addition to the victims' services and rights listed in Sections 230.6.3 and 230.6.4, victims of identity theft should receive appropriate assistance for the unique circumstances of the crime. Assist victims of identity theft as follows:

- Refer victims to useful or relevant services specifically for victims of identity theft, including the Federal Trade Commission, and non-governmental organizations;
- Refer victims to relevant credit reporting services;
- Advise victims to file an individual police report;
- Advise victims to contact their telephone provider if they wish to block harassing calls or change a telephone number; and
- Provide victims with the TIGTA identity theft brochure, *Victim Assistance Related to Identity Theft*, as applicable.

230.9.1 Identifying Direct Harm for Identity Theft Victims. If the suspect possesses an individual's Personally Identifiable Information (PII), determine through the investigative process whether the PII was used in a way that could cause harm to the individual. If no evidence indicates the information was misused, generally there is no "direct harm" to support victim status under the applicable Federal statutes (34 U.S.C. § 20141 and 18 U.S.C. § 3771).

If the PII was used by the suspect or others in committing a crime, determine whether the individual suffered direct harm as a result of the misuse. Direct harm in this type of case is typically financial harm, and could include out-of-pocket losses as well as time spent to remedy the situation. It is rare for an identity theft victim suffering solely from emotional harm to have victim status under the applicable Federal statutes, noted above. However, it is possible in extraordinary circumstances (*i.e.,* harm to one's reputation from a false arrest directly resulting from the misuse of the victim's PII).

See the 2011 AG Guidelines - Rev. May 2012, Article III, D, 3 for additional guidelines in assisting these victims.

230.10 Foreign Victims.
VRRA and CVRA rights and services for victims apply to foreign nationals meeting the definition of a victim, regardless of whether they reside in the U.S. or not. However, some countries prohibit or limit direct contact by foreign government officials with their citizens, thus requiring an intermediary contact.

Coordinate any contact with victims and witnesses residing in other countries through DOJ Office of International Affairs (OIA) or the appropriate U.S. attaché in the country where the victim/witness resides. The attaché can address foreign protocol, conduct or facilitate interviews, ensure concerns are addressed, and coordinate the services of a translator, if necessary.

230.11 Temporary Protective Measures.
OI may undertake temporary protective arrangements to protect victims/witnesses whose continued cooperation/testimony is essential to an investigation. Such temporary arrangements are not intended to replace DOJ's Witness Security Program.

Any protective arrangements undertaken by OI for a victim/witness not enrolled in DOJ's Witness Security Program require the approval of the appropriate Assistant Inspector General for Investigations (AIGI).

Note: SAs are not authorized to commit any funds for compensation and expenses of witnesses or confidential sources (CS), and are not authorized to make protective maintenance agreements.

230.11.1 Securing Approval for Temporary Protective Services. SAs shall immediately notify their SAC and DVWC of any threat or possible danger to a past or present Government CS, witness, or his/her family or close associate(s), as a result of his/her furnishing information or otherwise cooperating with OI. If the SAC determines if any protective arrangements are necessary and appropriate under the circumstances, the DVWC will contact the NVWC. In the event of immediate danger or emergency, SAs are authorized, with the approval of the authorizing official for confidential funds, to provide temporary measures until appropriate additional measures as follows can be taken:

- SACs are authorized to approve all confidential expenditures for temporary protection of a witness or CS for $2,500 or less;
- AIGIs and the Deputy Assistant Inspector General for Investigations (DAIGI) are authorized to approve all confidential expenditures for temporary protection of a witness or CS for $20,000 or less; and
- The Deputy Inspector General for Investigations (DIGI) is authorized to approve all confidential expenditures for temporary protection of a witness or CS of more than $20,000.

See TIGTA Operations Manual Chapter 600, Section 50.9.5.3, *Expenditures for the Protection, Relocation, and Maintenance of Witnesses,* and Chapter 600, Section 50.9.7, *Authorization to Incur Confidential Expenditures.*

See TIGTA Delegation Order No. 27.

230.11.2 Approval Memorandum for Temporary Protective Services. The SAC sends a memorandum requesting approval for the protection and maintenance of the affected person to the Operations Division e-mail box for review and approval by the appropriate AIGI, DAIGI, or DIGI, at *TIGTA Inv Operations. The following information shall be provided in the memorandum to the extent possible:

- Name, address, place and date of birth, gender, race, citizenship, and any identification numbers, such as Social Security Number, FBI or police numbers, on persons for whom protection is requested. Also, attach a copy of any record of arrest and/or conviction of the protected party;
- All facts and circumstances relating to the threat or danger to the CS or witness and family member(s) or close associate(s);
- Include the complete names and addresses of all individuals known or believed to pose a threat and their photographs, if available;
- Information and/or evidence supplied by the witness or CS, and the importance of the material;
- The involvement of the CS or witness in illegal activity;
- The importance and significance of the case and prospective defendants. If applicable, describe any illegal organization in which the defendants participate and their roles. Also, include each defendant's arrest and/or conviction record, if any;
- All other agencies to which the CS or witness has supplied, or is supplying, information, and any resulting cases;
- All pending cases, Federal or State, in which this witness' testimony may be required;
- Name of all individuals, CS, or witnesses who have been provided protection in connection with the same case; also, the names and locations of any other individuals connected with the case who are likely to be placed in DOJ's Witness Security Program or who are likely to require protection by TIGTA;
- Realistic estimate of the extent and duration of protective measures;
- Whether or not the witness appears to qualify for the DOJ's Witness Security Program;
- Number of family and/or household members to be protected, (*e.g.*, name, date and place of birth, and relationship; provide the same information for any close associates to be protected);

- Assets and liabilities of the protected party, such as property, loans, alimony, support payments, bank accounts, pensions, Federal, State, or local taxes, etc.;
- Medical problems/conditions experienced by the CS or witness and family/household members, and any history of drug abuse;
- Employment data (*e.g.*, education, job skills, last employment, and employability of individuals to be protected);
- Income from all sources;
- Whether the CS or witness is receiving, or expects to receive, money from other State or Federal agencies, and if so, how much;
- If the CS or witness is incarcerated, when release can be reasonably anticipated;
- Indicate any parole or probation restrictions on the CS or witness and family members or close associates;
- Expected expenditures and the reason, such as relocation, rent, etc.; and
- Location (*i.e.*, field division) of imprest fund to be utilized.

230.11.3 Conference with Protected Witness or Confidential Source. In all situations in which TIGTA assumes the protection of a witness or CS, SACs shall brief the CS or witness and document the following:

- OI contact/control personnel;
- Communications;
- Protection;
- Relocation;
- Subsistence arrangements being undertaken;
- Responsibilities of OI; and
- Responsibilities of the witness or CS.

Document that the CS or witness understands that any protection or subsistence afforded by OI is solely for his/her physical welfare and no compensation will be provided for:

- Loss of income;
- Personal inconvenience; and
- Any other type of monetary damage suffered, such as a distress sale of a business or residence.

230.11.4 Memorandum of Understanding. The NVWC, in consultation with TIGTA Counsel, obtains a signed memorandum of understanding (MOU) from the CS or witness, which documents the items discussed at the conference. The CS or witness must sign the MOU certifying that he/she fully understands and agrees with the terms and conditions set out in the agreement.

230.11.5 Accounting for Protection Expenses. Authorized confidential expenditures made for protection and maintenance provided by OI are accounted for in accordance with investigative imprest fund policy and procedures in Chapter 600, Section 50.9, of the TIGTA Operations Manual.

To avoid jeopardizing the new identity of the relocated witness or CS, maintain detailed information on these expenditures in the appropriate divisional investigative imprest funds files. Do not furnish detailed information to Fiscal Management offices. Claim reimbursement for confidential expenditures only through investigative imprest funds, not on travel vouchers.

230.12 Witness Security Reform Act of 1984.
DOJ's Witness Security Program is codified in the Witness Security Reform Act of 1984, primarily 18 U.S.C. § 3521. Under this act, the Attorney General may provide for the relocation and other protection of witnesses, or potential witnesses, in an official proceeding concerning organized criminal activity or other serious offenses. The Attorney General may also provide for the relocation and other protection of the immediate family of, or a person otherwise closely associated with, such witness or potential witness, if the family member or person may also be endangered on account of the witness' participation in the judicial proceeding. This protection may be authorized for Federal or State offenses.

An individual may not be the subject of protective appropriations from DOJ and OI at the same time. If DOJ deems an individual worthy of protection under the Witness Security Reform Act of 1984, TIGTA appropriations will cease when DOJ appropriations begin.

230.12.1 Eligibility for Witness Protection. Protection and maintenance are allowed upon the finding of DOJ's Director, Office of Enforcement Operations (OEO) that the proposed witness meets all of the following conditions:

- The person is a qualifying witness in a specific case;
- Evidence in possession indicates that the life of the witness, a member of his/her family, or a close associate is in immediate jeopardy; and
- Evidence in possession indicates it would be advantageous to the Federal interest for DOJ to protect the witness, family member, or close associate.

SAs who believe that a victim/witness should be enrolled in DOJ's Witness Security Program shall immediately notify the ASAC and the DVWC, who will consult the NVWC. SAs shall notify the ASAC and the DVWC any time an enrollee in DOJ's Witness Security Program becomes a victim/witness in a crime under investigation by OI. The DVWC will notify the NVWC of such situations as soon as possible.

230.12.2 Enrollment in DOJ's Witness Security Program. If a witness appears to qualify for the Witness Security Program, and there is no DOJ involvement, the DIGI coordinates the matter with OEO. The DIGI advises the SAC and NVWC of the appropriate action to take in order to continue or terminate any protective arrangements. Thereafter, a United States Marshals Service (USMS) representative will accompany an OI representative to meet the witness and to explain the scope of the Witness Security Program. Forward results of this preliminary meeting to the Director, OEO, for evaluation and determination. In situations where DOJ is already involved, refer to Section 230.12.4.

Information the Director, OEO may consider in determining whether enrollment in the Witness Security Program is appropriate includes, but is not limited to:

- The individual's criminal record;
- Alternatives to providing protection;
- Other possible sources of testimony; and
- The results of a psychological examination by psychologists from the Bureau of Prisons (BOP).

If it is determined that the witness is eligible for enrollment in the Witness Security Program, there will be a second meeting with the witness, at which time a MOU will be executed between the witness and the USMS.

230.12.3 United States Marshals Service Responsibility. The USMS is responsible for the protection and maintenance of witnesses and other qualifying individuals enrolled in DOJ's Witness Security Program.

230.12.4 Coordination with U.S. Attorney for Witness Protection. If the case is under the jurisdiction of a USAO, it is incumbent upon each U.S. Attorney, his/her assistants, and the investigative agency to present to the Director, OEO, as early as possible during the investigation process, the request for authorization to place an individual in the Witness Security Program. Therefore, the SAC shall provide the USAO any assistance necessary in developing the request. The SAC shall also follow the procedures in Section 230.11 of this section if any temporary protective arrangements are necessary. The assistance shall include:

- Working with the USAO to avoid unnecessary duplication of effort;
- Documenting in the approval memorandum that the USAO requested that the individual be placed in the Witness Security Program and the U.S. Attorney's involvement; and
- Protecting a witness for whom relocation is being requested until the Director, OEO, approves admission of the witness into DOJ's Witness Security Program and the USMS has arranged for the safe removal of the witness and his/her family or close associates.

230.12.5 Contacts After Acceptance into DOJ's Witness Security Program. Once a witness has been accepted into DOJ's Witness Security Program and is under the USMS jurisdiction, all contacts with the witness must be made through the USMS. Coordinate any necessary contact through the OI NVWC.

Occasionally, witnesses who have been provided protection by the DOJ are faced with a situation in which they believe their new identity may be in jeopardy because of the need to provide an OI employee with information relating to a witness' old identity. In such situations, the witnesses have instructions to notify their contact point in the USMS, who will notify the Director, OEO. The Director, OEO, will notify the OI NVWC to resolve the matter in a manner that will protect the CS' identity as well as OI's interest.

The above procedures are followed if during the processing of a witness to be placed in DOJ's Witness Security Program, the Director, OEO, determines that the witness has an OI matter that needs to be resolved before the witness is relocated.

Note: The DIGI may contact the Director, OEO, directly in emergency or other unusual circumstances involving an OI witness who is in DOJ's Witness Security Program.

230.12.6 Use of Relocated Witnesses. The DOJ maintains a continuing relationship with a person in the Witness Security Program after relocation. Because of this relationship, DOJ requires that investigative agencies and attorneys observe certain restraints in dealing with these persons insofar as new investigations and/or cases are concerned. The restraints are as follows:

- Once an individual has been placed in the Witness Security Program, neither the witness nor any individual relocated because of the witness' cooperation, may be used as a CS unless OI can justify to the Director, OEO, that the use of the individual as a CS is essential to the investigation.

- Without the consent of the Director, OEO, neither the witness nor any individual relocated because of his/her cooperation, may be used as a witness in a case other than the one for which the witness was placed in the Witness Security Program.

Once it is learned or suspected that a person is a protected witness, the SAC seeking to contact the witness will submit a memorandum to the Operations Division e-mail at *TIGTA Inv Operations requesting the DIGI contact DOJ to determine whether the person is actually a protected witness in the Witness Security Program. If the potential witness is enrolled in the Witness Security Program, the Director, OEO, must approve the person's participation in the OI investigation.

The memorandum must include:

- A brief explanation of the person's importance to the investigation;
- Whether it is anticipated that the person will be called to testify before a grand jury or at a trial; and
- Any other information that is relevant to a determination by the Director, OEO.

Until approval is obtained from the Director, OEO, OI will suspend its use of this person as either a CS or a witness. The use of a relocated witness by OI without the approval of the Director, OEO, could result in OI becoming responsible for the physical and financial security of the witness.

230.12.7 Federal Prisoners. The DIGI must obtain the approval of the Director, OEO, prior to any OI contact with a protected witness who is a prisoner at a Federal correctional institution. See Section 150.3.14.

If it is learned that an incarcerated, protected witness may be in jeopardy, provide immediate notice to BOP, with subsequent written notification to the Operations Division e-mail at *TIGTA Inv Operations. Notification should go through the appropriate AIGI to the DIGI. The DIGI is required to refer the matter to the Director, OEO.

DATE: April 1, 2021

CHAPTER 400 – INVESTIGATIONS

(400)-240 Processing Complaints, Reports of Investigation, and Congressional Inquiries

240.1 Overview.
This section details the procedures the Treasury Inspector General for Tax Administration's (TIGTA) Office of Investigations (OI) follows for receiving and processing complaints:

- General Guidelines for Receiving Complaints
- Complaints Received by the Complaint Management Team
- Complaints Received by Divisions
- Processing Complaints Referred by Internal Revenue Service Management to Office of Investigations
- Section 1203 Complaint Processing
- Reports of Investigation
- Section 1203 Complaints Received Directly by Complaint Management Team
- Section 1203 Complaints Received by Divisions
- Processing Reports of Investigation
- Processing Congressional Inquiries
- Processing *Qui Tam* Complaints

TIGTA's OI has established and publicized the toll-free hotline telephone number 800-366-4484 to receive complaints.

240.1.1 Acronyms Table.

240.2 General Guidelines for Receiving Complaints.
A **complaint**, as defined in this Section, is any allegation of criminal or administrative misconduct, mismanagement, or other impropriety within TIGTA's oversight purview of Federal tax administration, including allegations of misconduct by employees of the Internal Revenue Service (IRS), the Office of Chief Counsel of the IRS, the IRS Oversight Board, or TIGTA. An **intake** is the method by which complaints received by OI are recorded in CRIMES.

The **complainant**, as defined in this Section, is the person who initially reports the allegation. It does not refer to the source of the intake, which in many instances may be an intermediary that refers the initial information to TIGTA.

OI will assume ownership of all complaints, as defined in this section, received directly from an individual complainant. OI does not assume ownership of all complaints

referred by IRS management. See Section 240.5 for more information on processing complaint referrals by IRS management.

Assuming ownership means that OI will:

- Document the allegation in the Criminal Results Management System (CRIMES) within 15 days of receipt;
- Enter allegations OI receives from a complainant as a complaint not a lead. A lead is an allegation developed internally, such as a proactive initiative, and not information received from an external source.
- If the subject of the complaint is unknown, title the complaint as: COMPLAINT RE and a description of the allegation. For example, if complainant JOHN DOE reports that he witnessed an unknown individual stealing government property from an IRS loading dock, the complaint would be titled "COMPLAINT RE THEFT OF GOVERNMENT PROPERTY" or similar wording, not "COMPLAINT OF JOHN DOE." Never include the complainant's name in the complaint title;
- Interview complainant except as authorized by this Section;
- Provide complainant with the TIGTA Reference Number (TRN);
- Determine appropriate disposition of the complaint; and
- Document actions resulting from the complaint.

Upon identification of the subject, immediately update the appropriate sections of CRIMES and change the title of the appropriate referral forms to reflect the known subject's name.

OI divisions evaluate all complaints and makes a determination as to whether OI will initiate an investigation into the matter or take other appropriate action. The evaluation of complaints must be limited to preliminary inquiries to determine if the allegation(s) is within TIGTA's jurisdiction. If a decision is made not to open an investigation, the proper reason will be documented in the "Reason for no investigation" data field of the CRIMES intake screen.

Complaints received by OI employees that are within TIGTA's jurisdiction must be properly documented in CRIMES.

Information developed from internal initiatives, such as Fraud and Schemes Division, Unauthorized Access, integrity projects, or spin-off cases relating to multi-subject investigations, are documented as leads created from a master case in the CRIMES intake section and should not be entered via an intake as a complaint received by TIGTA.

Once a complaint is received and entered into CRIMES, TIGTA will contact the complainant to advise that TIGTA has received the complaint and to provide the TRN.

If there is an e-mail address associated with the complainant contact in CRIMES, the system will automatically e-mail them the TRN. CRIMES only sends the e-mail when an e-mail address is associated with the complainant when the complaint is created. If an e-mail address is added after the complaint was created, provide the TRN separately.

OI personnel will make reasonable attempts to interview all complainants, either telephonically or in person, within 15 days of receiving the complaint. The appropriate Assistant Special Agent in Charge (ASAC)/Assistant Director (AD) will approve any determination not to interview the complainant for those complaints received by divisions, or referred to a division by the Complaint Management Team (CMT), if CMT personnel did not previously conduct an interview. If a decision is made not to interview the complainant, document the reason in CRIMES, along with a statement indicating the Special Agent in Charge's (SAC)/Director (DIR) concurrence with the decision in the "Remarks" section of the CRIMES intake section. CMT is exempt from this recordation requirement.

TRNs are the only reference number authorized to be provided to a complainant. **OI personnel should never disclose the existence of an investigation by any means, including providing an investigation number**.

If possible, notify the complainant that his/her complaint has been referred to TIGTA for any complaint referred and accepted by OI from another agency (*e.g.*, complaints initially received by the IRS and subsequently referred to TIGTA).

Due to Federal privacy laws, OI generally will only advise a complainant that TIGTA has received the complaint. TIGTA generally cannot provide a complainant with information on his/her complaint unless requested pursuant to the provisions of the Freedom of Information Act (FOIA) and/or the Privacy Act. FOIA and Privacy Act requests are processed through the TIGTA Disclosure Branch. See Chapter 700, Sections 60 and 70, of the TIGTA Operations Manual for information concerning FOIA and Privacy Act requests.

For all complaints input into CRIMES, a SharePoint folder is automatically created. This SharePoint folder will be the only repository for the intake record and contain all documents that relate to the intake to include:

- Documents received from the complainant;
- TIGTA Forms OI 2028-M, *Memorandum of Interview or Activity*;
- TIGTA Form OI 2070, *Complaint Referral Memorandum (Response Required)* or TIGTA Form OI 2070-A, *Complaint Referral Memorandum (Referred for Information Only)*; and
- Legible scanned copies of the investigator's notes.

If the complaint is closed to file or referred for information only, document the reason why TIGTA chose not to investigate the complaint in the appropriate data field of the CRIMES intake section.

Hard-copy complaint notes may be destroyed once a legible copy has been scanned and retained in the SharePoint folder associated with the intake and the complaint is closed and/or referred.

240.3 Complaints Received by the Complaint Management Team.
The CMT will maintain a staff of Investigative Specialists (IS) that are available to receive complaints Monday through Friday, from 8:30 a.m. until 4:00 p.m. eastern standard time, excluding Federal holidays.

The CMT will maintain the capability to receive complaints through each of the following methods:

- Hotline telephone: 800-366-4484;
- Fax: 202-927-7018;
- U.S. mail: Treasury Inspector General for Tax Administration
  Hotline
  P.O. Box 589
  Ben Franklin Station
  Washington, DC 20044-0589;
- Internet: http://www.tigta.gov;
- Inter-office or Treasury Bureau routing; and
- E-mail: Complaints@TIGTA.treas.gov

When CMT receives a complaint, via a live call, through the Hotline, the receiving IS will conduct an interview of the complainant, if the complaint is within TIGTA's jurisdiction. The IS will enter the complaint into CRIMES, via an intake, unless the complaint is against a TIGTA employee. If the complaint is against a TIGTA employee, the SAC-Special Investigations Unit (SIU) is responsible for entering the complaint in CRIMES intake section.

If a complaint is received by other than a live call, the IS will enter the complaint in the CRIMES intake section and contact the complainant to develop additional information if necessary. The receipt of complaints and subsequent investigative activities will be recorded in accordance with Section 250.6. In circumstances where CMT receives an e-mail complaint that is immediately identified to fall within the jurisdiction of a specific division, forward the e-mail to the responsible SAC/Director, without inputting the complaint into CRIMES, for action as deemed appropriate.

For all complaints CMT enters into CRIMES, the AD-CMT or his/her designee, will send the complainant a written acknowledgement advising that TIGTA has received the

complaint, and provide the complainant with the TRN. In circumstances where an e-mail address of the compliant is entered in CRIMES, an automatic e-mail acknowledgement containing the TRN is sent to the complainant.

The AD-CMT or his/her designee will review the complaint for final disposition.

240.3.1 Complaint Management Team Referrals for Investigative Determination. If the AD-CMT determines the complaint involves alleged criminal violations within TIGTA's jurisdiction or a named IRS/TIGTA employee, CMT will refer the complaint to the appropriate SAC for an investigative determination as follows:

- CMT will refer any complaint involving the following to the SAC-SIU for an investigative determination:
  - Any IRS senior executive service (SES) official or IRS International employee;
  - IRS Criminal Investigation ASAC, SAC, and/or SES member;
  - Any allegation of fraud relating to the administration of TIGTA contracts; and
  - Any TIGTA employee.

- CMT refers any complaint involving the respective SAC-Division for investigative determination. CMT should:
  - Refer to the SAC-South East Field Division an IRS employee in the International (U.S. Competent Authority) function and located in Puerto Rico or the U.S. Virgin Islands.
  - Refer to the SAC-Western Field Division an IRS employee in the International (U.S. Competent Authority) function and located in Guam or the American Samoa Islands.
  - Refer all other complaints to the SAC covering the geographic area where the subject of the complaint is employed (if an IRS employee), or where the subject of the complaint lives, or where the alleged violation occurred (if a non-IRS employee).
  - Refer the complaint to the SAC who is responsible for the area where the complainant resides if a geographic area is not initially identified (*e.g.*, unknown subject).

- CMT will refer any complaint involving allegations of fraud relating to the administration of IRS/TIGTA contracts to the SAC-SIU, for an investigative determination.

When CMT personnel interview complainants, include a TIGTA Form OI 2028-M documenting the interview, then upload the form to the CRIMES SharePoint folder for the intake.

Upon receipt of the complaint, division personnel will make reasonable attempts to conduct a thorough complainant interview, either in-person or telephonically. See Section 240.4.

If a decision is made not to open an investigation, document the reason in the "Reason for no investigation" field of the CRIMES intake section. The SAC or his/her designee is responsible for making final disposition decisions regarding complaints.

240.3.2 Complaint Management Team Referrals to the Internal Revenue Service.
Forward all complaints that are referrals to the IRS's Employee Conduct and Compliance Office (ECCO) within 30 days, using the appropriate referral form. CMT will update the CRIMES intake section as appropriate. Referrals should sent to the IRS via SharePoint.

Outlined below is the contact information for ECCO:

Internal Revenue Service
Employee Conduct and Compliance Office
1111 Constitution Avenue, NW
OS:HC:R:EC:EI:ROIU, NCFB-C1-530
Washington, DC 20224

Fax number: 202-317-6287
Telephone number: 202-317-6929
E-mail: *HCO ECCO EAU

Process all complaints involving § 1203 violations in accordance with Section 240.6.

240.4 Complaints Received by Divisions.
Forward all complaints division personnel receive to the appropriate ASAC for evaluation and disposition. Division personnel will process complaints within 30 days of TIGTA's receipt of the complaint. This 30-day processing period includes reassignment of complaints from one division to another division.

Divisions will refer complaints to respective SACs for an investigative determination. Any complaint involving the following:

- Refer to the SAC-South East Field Division an IRS employee in the International (U.S. Competent Authority) function and located in Puerto Rico or the U.S. Virgin Islands.
- Refer to the SAC-Western Field Division an IRS employee in the International (U.S. Competent Authority) function and located in Guam or the American Samoa Islands.
- Refer all other complaints to the SAC covering the geographic area where the

subject of the complaint is employed (if an IRS employee), or where the subject of the complaint lives, or where the alleged violation occurred (if a non-IRS employee).
- Refer the complaint to the SAC who is responsible for the area where the complainant resides if a geographic area is not initially identified (*e.g.*, unknown subject).
- When a complaint does not warrant an investigation, make a referral to the SAC/ASAC for evaluation and disposition, and document the reason in the "Reason for no investigation" field of the CRIMES intake section.

If an investigation is not initiated, generally dispose of the complaint in one of the following ways:

- If the complaint involves issues where there is a potential for disciplinary action against one or more IRS employees, the originating SAC will forward it directly to ECCO for appropriate inquiry and response, via TIGTA Form OI 2070. Refer complaints involving IRS Chief Counsel employees to IRS Chief Counsel via SharePoint.
- Update the CRIMES intake section as appropriate. The IRS response to the complaint should include any actions taken and the scope of their inquiry into the matter. If the IRS response is lacking any of these elements, the originating SAC is to follow-up with the IRS to obtain the missing information. The CRIMES Coordinator will follow-up with ECCO on all complaints referred via TIGTA Form OI 2070 that are not returned within 180 days to ascertain the reason and anticipated date of response.
- Forward complaints that involve issues relating to IRS operations or personal/business tax, and there is no potential for disciplinary action against an IRS employee, or any other reason to track the IRS disposition of the complaint, to ECCO via TIGTA Form OI 2070A. Update the CRIMES intake section as appropriate.
- Forward by letter from the SAC to the agency having jurisdiction over the matter, complaints that are not under the jurisdiction of TIGTA or the IRS, as authorized by law. Update the CRIMES intake section as appropriate.
- The intake may be associated with a previously initiated and/or closed intake or investigation if the referred matter involves the same issue(s)/allegation(s). Update the CRIMES intake section as appropriate.
- The complaint may be documented in the CRIMES intake section as a non-actionable item (*e.g.,* closed to file).
- OI personnel must immediately forward any complaint or request for information from a member of the U.S. Congress to the Operations Division, Policy Team for appropriate response and tracking. If the SAC determines an immediate investigation of the matter is appropriate, he/she will coordinate with the SAC-Operations Division.

240.4.1 Lost Identification Media and Access Cards.

IRS issues various types of identification media and/or access cards to individuals affiliated with the IRS (*e.g.,* employees, contractors, volunteers). These cards may include a Homeland Security Presidential Directive 12, or Smart Identification Card (Smart ID), non-photo ID, or access card (*e.g.,* physical access control card, proximity card). If the identification media and/or access card(s) are lost or stolen, the cardholder is required to report its loss to the IRS Computer Security Incident Response Center or the IRS Situation Awareness Management Center, and TIGTA.

Although all types of losses may not require a referral, the IRS requires the cardholder who lost the card (the complainant) to obtain a TRN prior to issuing a replacement. To address this challenge, a SharePoint site was created to capture information relating to the loss, which generates a "Loss Number" in the same format of a TRN. The loss number is four digits for the fiscal year of the loss, followed by four digits to correspond to the loss number, for example, 2020-0001, 2020-0002, etc.

Document all complaints via OI's Lost ID Tracker SharePoint site regarding lost identification media and access cards **excluding the exceptions indicated below**. In these circumstances, no complainant interview is required. The receiving OI employee must capture the following information:

- Date of loss;
- Complainant's First and Last Name;
- Affiliation (*e.g.,* Employee, Contractor, Volunteer);
- Type of Loss;
- Type of identification lost;
- Standard Employer Identifier (SEID); and the
- City and State of the complainant's post-of-duty.

SEID's are not required for volunteers.

The following **exceptions** apply to the abbreviated process outlined above. If the identification media and/or access card was:

- Found at a crime scene;
- Used in the commission of a crime or other serious misconduct;
- Used by someone else to gain access to a facility or information technology system; or
- Used to provide access to classified material.

Complaints meeting the criteria above require a CRIMES intake entry, and a complainant interview. Document the tracking of lost or stolen media by a national investigative initiative.

240.5 Processing Complaints Referred by Internal Revenue Service to Office of Investigations.
Generally, OI will receive complaints from IRS in two ways: referrals by IRS directly to an OI division, or by ECCO referral to CMT. In all instances, the receiving OI employee will document receipt of the complaint in the CRIMES intake section.

In most instances, OI will not take further action on complaints referred by the IRS that are limited to allegations concerning:

- Rude or unprofessional conduct on the part of an IRS employee;
- IRS management competence or judgment issues;
- Personnel or labor relations issues;
- Taxpayers' personal or business tax issues;
- IRS systems/process issues; or
- Legality of tax system issues.

However, consideration should always be given to making a referral to TIGTA's Office of Audit or Office of Inspections and Evaluations when programmatic or systemic issues are present.

In instances where OI takes further action on a complaint received by a non-employee, OI will notify the complainant advising him/her that TIGTA has received his/her complaint and provide the complainant with the related TRN.

240.6 Section 1203 Complaint Processing.
Complaints and investigations involving alleged violations of § 1203 of the Internal Revenue Service Restructuring and Reform Act of 1998 (RRA 98) will receive special processing, as they are tracked and adjudicated differently than most other types of misconduct. Generally, TIGTA will initiate an investigation into all bonafide complaints that allege a § 1203 violation. Usually, the only exceptions will be § 1203(b)(8) and (b)(9) allegations, which relate to timely and full payment of taxes. In some instances, the IRS, if requested to conduct a preliminary inquiry into these § 1203 allegations, may fully resolve the issues and not warrant a TIGTA investigation.

The SAC/ASAC will review the complaint to determine if there is a basis for a § 1203 allegation. For there to be a basis for a § 1203 allegation, the following should be apparent in the complaint:

- The complaint alleges misconduct by an IRS employee, whose identity may either be known or unknown; and
- The substance of the allegation relates to one or more of the 10 specified § 1203 violations. See Exhibit (400)-240.1 for the RRA 98 § 1203 Plain Language Guide to determine the elements for a specific § 1203 violation.

In some instances, the date that the incident occurred may not be readily apparent in the complaint and will require an interview of the complainant to determine when the incident on which the complaint is based actually occurred.

If the SAC/ASAC determines that the two criteria above have been met, enter the complaint into the CRIMES intake section using the appropriate § 1203 violation code.

If the SAC/ASAC determines not to initiate an investigation, refer the complaint to ECCO for review by the Board on Employee Professional Responsibility (BEPR). The BEPR will include representatives of TIGTA, IRS National Headquarters, and the appropriate IRS operating division. If the BEPR recommends an investigation to resolve a § 1203 issue regarding the complaint, the TIGTA representative will determine whether to initiate an investigation.

Do not remove the § 1203 violation code from the CRIMES intake section when an IRS initial inquiry and evaluation determines there is no basis for the § 1203 allegation. Retain the § 1203 violation code in the CRIMES intake section due to special reporting requirements and analyses conducted at Headquarters.

A § 1203 violation code will not be removed from CRIMES by field division personnel once the code is entered, even if the subsequent investigation disproves or otherwise fails to substantiate the § 1203 allegation. Again, it is necessary that the § 1203 violation code be retained in the CRIMES due to special reporting requirements and analyses conducted at Headquarters.

240.7 Reports of Investigation.
Generally, TIGTA divisions will forward completed reports involving a § 1203 violation to ECCO, Employee Issues Branch, Report of Investigations Unit in accordance with the instructions contained in Section 250.12. If the investigation involves personnel identified in Section 340.2, the SAC-Division and the SAC-SIU will make an agreement on processing. The Remarks Section of TIGTA Form OI 2076, *Referral Memorandum*, must reflect the following statement: **"This report contains a § 1203 matter and must be forwarded to the ECCO Employee Issues Branch, Report of Investigations Unit."** This statement is needed to ensure that all investigations involving a § 1203 allegation are properly and timely routed to the BEPR and thereafter properly adjudicated.

240.8 Section 1203 Complaints Received Directly by the Complaint Management Team.
The CMT will review, evaluate, and document all direct intake of § 1203 complaints as appropriate in the CRIMES intake section.

If there are other serious misconduct or criminal issues that indirectly relate to the § 1203 violation, enter an intake into CRIMES and immediately refer the complaint to the appropriate SAC for an investigative determination of these non-Section 1203 issues.

For all other § 1203 allegations not relating to those listed above, if it is determined there is a basis for a § 1203 violation, forward the complaint directly to the appropriate SAC for investigation.

240.9 Section 1203 Complaints Received by Divisions.
The receiving special agent (SA) will review, evaluate, and document as appropriate in the intake section within CRIMES all § 1203 complaints the division receives.

The receiving SA will then forward the complaint to his/her ASAC/AD for review and a disposition determination.

If the complainant specifically alleges a § 1203 violation, but the SAC/ASAC determines there is no basis for the § 1203 allegation, then forward the complaint to ECCO on TIGTA Form OI 2070.

If the complaint alleges a § 1203 violation and the ASAC determines there is a basis for the § 1203 allegation, then he/she will initiate an investigation, except as provided below.

If one of the following § 1203 violations is alleged:

§ 1203 (b)(1)	§ 1203 (b)(3)(B)	§ 1203 (b)(8)
§ 1203 (b)(3)(A)	§ 1203 (b)(6)	§ 1203 (b)(9)

The SAC/ASAC may send the complaint package to ECCO for initial inquiry and evaluation as to whether there is a basis for a § 1203 violation.

However, the SAC may elect to investigate any alleged § 1203 violation without referral to the IRS for initial inquiry and evaluation.

For those complaints referred to ECCO for initial inquiry and evaluation, if the IRS determines there is no basis for the § 1203 allegation, then close the complaint upon return of TIGTA Form OI 2070 from the IRS.

For those complaints referred to ECCO for initial inquiry and evaluation, if the IRS determines there is a basis for the § 1203 allegation, then initiate an investigation upon return of TIGTA Form OI 2070 from the IRS. Initiating an investigation after referring a complaint to ECCO requires assistance and submission of a CRIMES helpdesk ticket.

240.10 Processing Reports of Investigation.
The originating SAC will forward reports in accordance with guidance contained in Section 250.12. An exception are reports with allegations against personnel identified in Section 340.2, which moves onward to SAC-SIU, who in turn will date TIGTA Form OI 2076 and forward it to ECCO, unless otherwise agreed by the SAC-SIU and the SAC-Division.

Upon completion of the adjudication process, the IRS adjudicating official will return the ROI and the accompanying TIGTA Form OI 2076 through ECCO to the referring SAC as documented on the TIGTA Form OI 2076.

If the adjudication process extends beyond 180 days for a particular case, the CRIMES Coordinator will follow-up with ECCO to determine the reasons and the anticipated completion date of the adjudicative actions. ECCO will advise the SAC of the appropriate IRS management personnel to contact regarding the matter. For cases forwarded to the IRS by SAC-SIU, SAC-SIU will be responsible for monitoring.

The IRS adjudicating official will document the TIGTA Form OI 2076 with any administrative actions taken, the date of the decision, and the Automated Labor and Employee Relations Tracking System issue code.

If the originating SAC believes the administrative action taken by the IRS is not commensurate with the results of the investigation and the issue cannot be resolved by the SAC with the IRS directly, forward the issue to the appropriate Deputy Assistant Inspector General for Investigations (DAIGI), Assistant Inspector General for Investigations (AIGI) and/or to the Deputy Inspector General for Investigations (DIGI), who may raise the matter to the Inspector General or the appropriate IRS executive responsible for the employee.

240.11 Processing Congressional Inquiries.
The TIGTA Congressional Affairs Liaison logs all congressional correspondence into the TIGTA Congressional Application. Forward all congressional inquiries requiring action by OI to SAC-Operations Division for initial documentation, assignment, coordination, and tracking.

Within the Operations Division, the Policy Team is responsible for initiating appropriate actions and sends timely response letters (acknowledgement and final response) to congressional representatives, for congressional inquiries responsive to OI. The Policy Team prepares congressional responses to individual Members of Congress in letter format for the signature of the DIGI and congressional responses to congressional committees in letter format for the signature of the Inspector General. The Operations Division ensures appropriate clearance (*e.g.,* Chief Counsel, Congressional Affairs Liaison) are obtained prior to providing a response letter to the signatory authority.

The Operations Division will simultaneously refer the congressional inquiry to the appropriate SAC for proper action and response to the Operations Division regarding results of the inquiry. The respective DAIGI and AIGI will receive a copy of the referrals to the divisions. Unless there are extenuating circumstances, and if applicable, the SAC will ensure that the constituent making the complaint is interviewed.

The SAC will endeavor to complete the inquiry or investigation in a timely manner, but usually within 30 days of receiving it from the Operations Division. In those instances, when the SAC is unable to complete the inquiry within the first 30 days after receiving the inquiry, the SAC will submit a status e-mail to the SAC-Operations Division via *TIGTA Inv Operations, respective DAIGI, and AIGI every 30 days until closure of the investigation. The status e-mail must contain a brief synopsis of the leads conducted and an estimated completion date.

In each status report, the SAC will advise the Operations Division whether the division anticipates completing the investigation within the next 30-day time period. If anticipation is the investigation will continue beyond the next 30 days, the SAC will include an explanation for the delay.

An “extension request” must be submitted in CRIMES, if completion of intakes or investigations cannot occur within the prescribed time period. The request is routed to the appropriate DAIGI or AIGI for approval. The case agent will receive notification of the approval via e-mail when the “extension request” is granted or denied. Extension requests are in addition to, and not a replacement for, status e-mails.

Update the intake or investigation referral recommendation when the SAC’s inquiry into the matter is complete. The submitting SAC will “approve” the referral recommendation in CRIMES. Prior to approving the referral recommendation, the SAC will ensure that all of the documents associated with the intake/investigation are stored in the CRIMES SharePoint folder.

Combine the finalized intake or investigation into a single .pdf document and title by the case number, the complaint or investigation, for example:

XX-XXXX-XXXX-CG.pdf
XX-XXXX-XXXX-I.pdf

Do not approve/forward intakes or investigations to the Operations Division without a complete .pdf in final format. If intakes or investigations are not submitted properly, the review task will be disapproved and returned to the originating SAC for correction.

The SAC’s approval of the intake/investigation in CRIMES will submit the intake/investigation to SAC-Operations and the ASAC-Policy for review. The inquiry will undergo a thorough review by the Operations Division and OI Executives, prior to

responding to the appropriate Member(s) of Congress or Committee. Upon receipt of final approval, the Operations Division will approve the task in CRIMES, and the submitting SAC will receive a notification/task in CRIMES of the action. The receiving SAC may then approve the intake/investigation for an appropriate disposition (*e.g.,* refer for action, adjudication).

240.12 Processing *Qui Tam* Complaints.
A *qui tam* complaint is a civil suit filed under the provisions of the False Claims Act by a private citizen in the name of the United States. The law requires filing of *qui tam* complaints under seal and that the Department of Justice (DOJ) receive a copy of the complaint. DOJ has 60 days, not including possible time extensions, to review the complaint and determine if they want primary responsibility for prosecuting the case.

When a *qui tam* complaint is filed involving the IRS or TIGTA, DOJ may ask TIGTA-OI to help with its review of the complaint. Upon receipt of a *qui tam* complaint, contact TIGTA Office of Chief Counsel for guidance and coordination with DOJ.

DATE: July 1, 2017

CHAPTER 400 – INVESTIGATIONS

(400)-250 Investigative Reports and Case File Procedures

250.1 Overview.
This section establishes the Treasury Inspector General for Tax Administration (TIGTA)-Office of Investigations (OI) policy regarding case file procedures, investigative reports and referrals.

250.1.1 Acronyms Table.

250.2 Case Numbering and Information Retrieval Systems.
The OI case numbering system in the Criminal Results Management System (CRIMES) is a uniform method for the identification, control, and accounting of investigations and complaints nationwide. See Section 80 of this chapter.

250.3 Official Case File.
All investigative activity should be recorded in an official case file. SAs must be diligent in maintaining case files in an orderly manner. Information contained in case files may be sought from TIGTA through discovery requests from parties in litigation or requested

by members of Congress and Congressional committees. Case files are also subject to release under the Freedom of Information Act (FOIA) and the Privacy Act.

250.3.1 Case File Procedures. Once an investigation has been entered into CRIMES and approved by the Assistant Special Agent in Charge (ASAC) or Special Agent in Charge (SAC), as appropriate, prepare and maintain the case file using the following procedures:

- File office of origin cases numerically by investigation number.
- File the initiation documents, including the CRIMES Case Tracking Sheet, on the left-hand side of the case folder.
- File Forms OI 6501, Chronological Case Worksheet, on the left-hand side of the case folder.
- File notes and completed Forms OI 2028-M, Memorandum of Interview or Activity chronologically on the right-hand side of the case folder.
- Maintain original tax return documents separately in a labeled envelope on the right-hand side of the case folder.
- Maintain any other original case-related documents not being placed into evidence in a labeled envelope on the right-hand side of the case folder.
- Maintain Forms OI 2028-M designated as grand jury information in a Form OI 6504, Restricted File on the right-hand side of the case folder. See Section 250.25 of this chapter for procedures regarding the protection of original grand jury documents.

250.3.2 Closed Case File. The closed case file includes:

- Form OI 6501;
- Original Form OI 2028R, Report of Investigation;
- Form OI 2028A, Exhibit List Sheet;
- Exhibits;
- CRIMES Case Tracking Sheet showing the closed case status;
- Investigative notes as defined in Section 250.5;
- Documentation of administrative actions, legal actions, financial accomplishments and other investigative results;
- Form OI 2076, Referral Memorandum if the report was referred for action and response or Form OI 2076-PDT, Assault/Threat Investigation Referral Memorandum, if applicable;
  Form OI 6504, if applicable, containing the removed grand jury pages from the report;
- Other formal documents such as memoranda, letters, and transmittals;
- Any approved operational plans (*e.g.,* Search Warrant, Armed Escort) or disclosure authorizations; and
- Fact Sheets (to include associated attachments).

The special agent (SA) should remove extraneous documents from the closed case file prior to forwarding to the Records Management Section (RMS).

See Section 250.25 of this chapter for closing and reporting grand jury cases and disposing of grand jury material.

250.3.3 Case File Retention Procedures. The SAC will retain the case file and original report in the field division until such time as all actions relating to the investigation have been completed. When all actions have been completed, the SAC or ASAC, as appropriate, will forward the closed case file via overnight courier to:

TIGTA – Office of Investigations
1401 H Street NW, Suite 469
Washington, DC 20005
Attn: Records Management Section

The SAC will not retain a division copy of the case file or the report.

Case files will be maintained pursuant to record retention schedules. See Chapter 600, Section 110 of the TIGTA Operations Manual.

250.4 Chronological Case Worksheet.
The Form OI 6501, Chronological Case Worksheet (CCW), is a sequential record of investigative steps taken during an investigation. It is also used to:

- Outline the initial investigative work plan; and
- Document the results of 90-day case reviews conducted by ASACs. *

The Council of Inspectors General on Integrity and Efficiency (CIGIE) has published "Quality Standards for Investigations" which includes general and qualitative standards for investigations. The CIGIE standards address the importance of timeliness of investigations.

The Form OI 6501 provides the SA, the ASAC and any other reviewer a ready reference to what has been completed and/or what remains to be accomplished in the investigation. SAs must take reasonable steps to avoid lapses in investigative activity to ensure that investigations are proceeding in a timely manner.

The Form OI 6501 is required to be created and updated in CRIMES. A separate Form OI 6501 is no longer acceptable unless it is to document grand jury activities.

*ASACs should annotate their case reviews by making an entry themselves into the electronic Form OI 6501. If he/she is serving as an Acting ASAC, the designation “Acting ASAC” should also be included.

250.4.1 Preparing the CCW. When an investigation is initiated, prepare a Form OI 6501. Complete the heading section on the form, provide a narrative of the allegations and list the relevant Federal criminal statutes and/or administration violations. After analyzing the allegations, enter the initial investigative work plan. Place the Form OI 6501 on the left side of the case file.

250.4.2 Investigative Work Plan. The case agent will develop an investigative work plan using the Form OI 6501. The investigative work plan is flexible and subject to change as the investigation proceeds. Consider the alleged violation(s) and the necessary elements of proof when developing the work plan.

Arrange to interview the complainant within 15 days after receiving the complaint, if feasible. Because the Privacy Act requires that information be collected "to the greatest extent practicable directly from the subject individual," discuss with the ASAC the practicality of conducting an upfront subject interview. Note the decision with a brief explanation. See Section 210.5 of this chapter.

When developing the investigative work plan, consider the following:

- What third-party witness interviews should be conducted?
- Are there any records to be reviewed (*e.g.,* IRS records, criminal histories, etc.)?
- How will the records be obtained?
- Will collateral leads need to be conducted?
- What other investigative steps should be conducted?
- Are any specialized techniques contemplated?

After preparing the Form OI 6501, discuss the investigative work plan with the ASAC within 10 days of receipt of the case. After discussing the work plan, the ASAC will approve the investigative work plan within 10-days of case initiation and reflect such approval on the Form OI 6501.

250.4.3 Documenting the CCW. Document all investigative activity on the Form OI 6501, including:

- The date the investigative activity was completed;
- A brief description of the investigative activity and results; and
- The date the Form OI 2028-M was prepared to document the lead/activity;

Investigative activity conducted by other TIGTA SAs and the date the 2028-M was prepared will be documented on the Form OI 6501. Do not include non-investigative activity (*e.g.*, annual or sick leave, working other investigations, detail assignments, etc.) on the Form OI 6501.

ASACs are responsible for noting any grand jury involvement on the Form OI 6501. This serves as a reminder to safeguard grand jury information.

250.4.4 CCW Procedures at Case Closing. After the investigation is completed, the ASAC enters on the CCW the date that he/she reviewed and forwarded the report of investigation or closed the case to file.

The original Form OI 6501 will be maintained in the closed case file that is forwarded to the Operations Division, RMS. See Section 250.3.1. ASACs may keep a copy of the Form OI 6501 for one year to aid in the ASAC's evaluation of the SA's performance.

250.5 Investigative Notes.
Investigative notes are prepared when planning and conducting investigative leads. They are used as records of interviews, investigative activities, observations, etc. Investigative notes assist the SA with the later recall of events and are used to prepare the Form OI 2028-M.

Investigative notes should be maintained in an orderly manner. Information contained in case files, including investigative notes, may be sought from TIGTA through discovery requests from parties in litigation or requested by members of Congress and Congressional committees. Case files, including investigative notes, are part of TIGTA's system of records and information contained therein may be subject to release under the Freedom of Information Act and the Privacy Act.

Investigative notes include:

- Handwritten notes, audio recordings, or other notes made during the course of, or contemporaneous with, an interview;
- Forms that require the witness or subject to acknowledge receipt of his or her rights (*e.g.,* IRS Form 8111, Employee Notification Regarding Union Representation; Form OI 8112, Statement of Rights and Obligations; IRS Form 9142, Employee Notification Regarding Third Party Interviews;);
- Notes prepared during surveillance activities, at searches and crime scenes, or other investigative activities which contain information that could be included in formal reports or are records of events about which the SA may later testify;
- Notes taken by an informant and given to an SA (every effort must be made to preserve the notes in the case file); and
- Diagrams, drawings, charts.

250.5.1 Handwritten Notes. Handwritten notes must be legible and made contemporaneous with the investigative activity. Properly identify persons interviewed, records reviewed, custodians, SAs conducting interviews or reviews, and the date of the activity.

250.5.2 Audio or Other Notes. Audio or otherwise recorded notes must be properly labeled with content, individual making the recording, and date of the recording.

Rough draft Forms OI 2028R or Forms OI 2028-M are not considered notes unless the rough draft is the SA's first written record of an interview or investigative activity. When this occurs, the rough draft itself becomes the SA's original notes and must be retained.

250.5.3 Retention of Notes. Retain all investigative notes made in conjunction with an investigation. Retain all administrative records of investigative activities and any documents that help protect the chain of custody of evidence or aid an SA's testimony at trial. Investigative notes are retained in the investigative case file forwarded to RMS. See Section 250.3.1 for case file procedures and Section 250.5 for investigative notes definition.

The SA should remove extraneous documents from the closed case file prior to forwarding to RMS. Documents that do not meet the definition of investigative notes should be destroyed after all criminal and adjudicative proceedings are completed, prior to the case file being forwarded to RMS.

250.5.4 Notes Procedures at Case Closing. Place all notes in an envelope for inclusion in the case file with the final report of investigation. When all administrative and/or criminal actions on the investigation are completed, the notes will be forwarded along with the original case file to the RMS. See Section 250.3.1 for case file retention procedures.

250.5.5 Collateral Report Notes. Submit collateral reports to offices of origin with investigative notes attached in a sealed envelope. See Section 250.10.

250.6 Memorandum of Interview or Activity.
The results of investigative activities (e.g., Allegation Received, Records Review, Interview) should be accurately and completely documented in the case file. Forms OI 2028-M, are complete records of investigative leads and activities conducted including interviews, record reviews, record checks, enforcement activities, prosecution referrals, etc.

250.6.1 Form OI 2028-M Timely Preparation. Prepare Forms OI 2028-M as soon as possible, but no later than 5 calendar days after conducting the leads. Timely preparation of investigative leads:

- Enhances the writer's ability to recall details of the activity; and
- Precludes a subject's assertion that the time lapse caused the SA to inaccurately recall and report the incident.

250.6.2 Form OI 2028-M Format. When reporting interviews, record reviews, record checks, or other investigative activity on Form OI 2028-M:

- Include the date and the name, address, and position of the person interviewed or furnishing the record.
- Reference all documents such as Privacy Act Notice – Employee Interviews (Privacy Act Notice 417), IRS Form 8111, Form OI 8112, and IRS Form 9142 that are provided to an interviewee on the Form OI 2028-M.
- Report interviews in the third person. Use first person only in direct quotes.
- Use capital letters when referring to the names of all principals and witnesses.
- Business names should not be written in all capital letters.
- Print all Forms OI 2028-M for inclusion in the case file.
- Report only one lead per Form OI 2028-M.

250.6.3 Documenting Interviews of Third-Party Witnesses. When preparing Forms OI 2028-M to document interviews of third party witnesses in administrative investigations, document that the requirements of the Privacy Act of 1974, 5 U.S.C. § 552a (2013) were met; and, that all required and appropriate forms were issued.

250.6.4 Form OI 2028-M Retention. When Forms OI 2028-M are not pertinent or relevant to the investigation:

- Exclude them from the Report of Investigation and Exhibits; and
- Maintain them in the investigative notes.

250.6.5 Identifying Exhibits. A Form OI 2028-M should be prepared briefly summarizing the relevant information for every record check, document, etc., used as an exhibit. The Form OI 2028-M should also identify how, when, where, and from whom the document was obtained.

250.7 Report of Investigation.
The Form OI 2028Ris the standard format for reporting all investigations conducted by TIGTA-OI, except for collateral investigations. The Form OI 2028R should provide a brief and concise summary of information pertinent to the investigation. A typical Form OI 2028R can accomplish this goal in a two-page format. Forms OI 2028R that exceed two pages in length must be approved by the ASAC with the approval annotated on OI Form 6501.

250.7.1 Administrative Data. The Form OI 2028R will report the following administrative information:

- Case Title – include the subject's name and address if known.

- Type of Investigation – specify whether the investigation relates to “Employee,” “Non-Employee,” Local Investigative Initiative (LII), National Investigative Initiative (NII), or “TIGTA Employee.”
- Type of Report – use the blocks to designate “Final” or “Supplemental.”
- Subject’s Identifying Information (*e.g.*, Social Security Number, date of birth, date entered on duty (if Federal employee), and employment position and grade). Use the blocks marked for "Employee," "Non-Employee," or “Former Employee," to designate the employment status of the subject of the investigation.
- Post of Duty, if applicable.
- Division and Office, if applicable.
- Period of Investigation – include the dates of the first and last investigative steps. (The first investigative step should be the date the allegation was received by TIGTA).
- Potential Violation(s) – this block should specify the violation code(s) involved, and is populated automatically based on information contained in the PARIS-Investigations Screen, “S3 Violations.”
- Distribution – this block should indicate each entity receiving a copy of the Form OI 2028R.
- Date of Report – the date that the supervisory official approved and issued the Form OI 2028R.
- Use capital letters when referring to the names of all principals and witnesses.

The first page of Form OI 2028R is not numbered as page "1." Number pages sequentially beginning with "2" on the first continuation page, and continue sequentially until the end of the exhibits.

250.7.2 Investigative Synopsis. All Forms OI 2028R will contain an “Investigative Synopsis” section. Generally, this section summarizes the basis of the investigation, the investigative findings, and prosecutorial referrals. Do not prepare this section with a chronology of investigative steps. However, chronologies are acceptable when the order of events is significant, or best explains the development of evidence or proof of the elements of the offense. For example, the chronology in a series of bribery meets is pertinent.

250.7.2.1 First Paragraph of Investigative Synopsis. The first paragraph of the “Investigative Synopsis” will briefly describe the basis for the investigation. This paragraph will:

- Include the date the allegation was received by TIGTA;
- Identify the source of the allegation;
- Briefly describe the allegation (if using a quotation, be sure to quote verbatim); and

- If the source of the allegation provided any documents, attach the documents as an exhibit.

Information contained in the first paragraph of the "Investigative Synopsis" of the report should be the same as that documented in the "Basis" section within CRIMES.

250.7.2.2 Subsequent Paragraphs of the Investigative Synopsis. Subsequent paragraphs within this section will summarize pertinent information which best describes the activities in the case. State the activities that substantiate or disprove the allegations. Support all information in this section with an exhibit.

If other allegations are developed during the investigation, the narrative will indicate the nature and source of the additional allegations developed. For example, a developed allegation would be introduced in the Investigative Synopsis as "During the course of the investigation, TIGTA received an allegation that…"

250.7.2.3 Documenting Referrals. All formal criminal referrals, to include those made pursuant to a blanket declination agreement, will be noted in the "Investigative Synopsis."

For cases referred to the IRS for information only, this section will contain a statement as to the reason the case is being referred for informational purposes.

For cases closed without referral, this section will contain a statement as to the reason the case is not being referred for criminal, administrative, or civil action.

250.7.2.4 Documenting Results. Forms OI 2028-R will not document whether an allegation was "substantiated," "disproved," or "unresolved."

250.7.3 Exhibit List Sheet. TIGTA Form OI 2028A, Exhibit List Sheet, precedes the exhibits contained in the Report of Investigation. The Form OI 2028A identifies all exhibits that are part of the report. Include the case title and number in the footer of the page.

250.7.4 Exhibits. Exhibits contain all relevant evidence which substantiates, disproves, or mitigates the allegation(s). Exhibits must support the information contained in the investigative synopsis.

Exhibits follow the Form OI 2028A. Exhibits include, but are not limited to:

- Forms OI 2028-M;
- Forms OI 8273 (required in all assault investigation reports);
- Affidavits;
- Records;

- Photographs;
- Relevant IRS and other forms; and
- Other documentary evidentiary material.

Note: Do not include internal TIGTA correspondence, TIGTA e-mail, or other TIGTA memoranda as an attachment or exhibit.

250.7.5 Exhibit Procedures. Whenever possible, place exhibits in the same logical order that the information is presented in the text of the Form OI 2028R. Follow these guidelines for exhibits:

- Number Forms OI 2028-M or cover sheets placed in the report to introduce exhibits.
- Include handwritten affidavits; if handwriting is not legible, also include a typed or letter-quality computer printed copy.
- A blank page entitled "See Restricted File Envelope" should be placed in lieu of the exhibit where that information would otherwise be located. See Section 250.25 of this chapter for closing and reporting grand jury cases.
- When return information and/or tax returns, including Integrated Data Retrieval System (IDRS) printouts, are attached as exhibits, include only the documents pertinent to the allegations.
- Documents provided to an interviewee such as Privacy Act Notice 417, IRS Form 8111, IRS Form 9142, Form OI 5230, and Form OI 8112 may be placed in the report as exhibits. These forms must be kept with the investigative notes in the case file if they are not included in the report as exhibits. See Section 250.6.2 regarding documenting forms provided to an interviewee.

Do not include the following materials in reports:

- Do not include information obtained from the Financial Crimes Enforcement Network (FinCEN), which contains Bank Secrecy Act information (e.g., Suspicious Activity Reports). Information obtained from FinCEN should be used as lead material only;
- IRS Automated Labor & Employee Relations Tracking System (ALERTS) printouts;
- CRIMES Indices Checks;
- Do not include police reports which are considered law enforcement sensitive documents. This information should be summarized and the review documented on a Form OI 2028-M; and
- Federal Bureau of Investigation (FBI) criminal history printouts such as National Crime Information Center (NCIC) or TECS generated documents. See Section 150 of this chapter for procedures on reporting TECS and NCIC information.

250.7.6 Report Security. Take precautions to prevent the disclosure of Reports of Investigation to unauthorized persons. Only authorized individuals with a need to know may access Reports of Investigation.

250.8 Cross-Indexing.
SAs are responsible for cross-indexing individuals and entities that are **substantively** involved in the investigation. Guidelines for cross-indexing are provided in Section 80 of this chapter. Cross-indexed names may be disclosed pursuant to Privacy Act or FOIA requests.

Cross-index items at the initiation, during, and at the completion of an investigation in CRIMES. All OI employees have access to information cross-indexed by other field divisions and offices, except for some information input into CRIMES by the Internal Affairs Division.

250.9 Supplemental Investigations.
IRS adjudication authorities may request that TIGTA furnish additional information or conduct further investigation on cases previously submitted for administrative action. If the ASAC determines that requests are feasible, he/she can authorize reopening of the case.

Report additional investigation on Form OI 2028R marking the space designated "Supplemental." The Supplemental Form OI 2028R and supporting documents will be maintained in the original case file.

250.10 Collateral Investigations.
Field divisions may request that another field division conduct a collateral investigation when investigative leads are outside of the office of origin's geographic area. The requesting field division is the office of origin. The field division that receives the collateral and completes the requested investigative steps is the receiving/reporting field division.

250.10.1 Collateral-Office of Origin. The office of origin ASAC is responsible for:

- Initiating the request;
- Following up on collateral requests; and
- Reviewing results for sufficient coverage.

The request for a collateral report can be made verbally, but should be followed up in writing via either memorandum or e-mail by the ASAC. A copy of the request should be maintained in the case file. The request should:

- Identify investigative factors to be covered;
- Provide special instructions; and

- Furnish additional information that may assist the receiving office.

250.10.2 Collateral Report. A collateral report consists of Forms OI 2028-M and exhibits/attachments, if any, conveying the results of the collateral inquiry and all investigative notes. Notes should be placed in a sealed envelope.

The receiving/reporting field division does not identify exhibits by exhibit number in the collateral report since they may be integrated into the office of origin report. The receiving/reporting field division retains a copy of the results of their investigation.

250.10.3 Receipt of Completed Collateral Investigations. The office of origin maintains the Forms OI 2028-M, notes and other documents from the receiving/ reporting field division in accordance with the guidelines in Section 250.3. The office of origin inserts the Forms OI 2028-M and other exhibits in a logical position in the report when it is prepared.

The office of origin ASAC should advise the receiving/reporting field division ASAC of the receipt of the collateral investigation. When the collateral receiving/reporting field division receives notification of the receipt of the collateral report by the office of origin, the receiving/reporting office should destroy the retained copy of the collateral report.

250.11 Special Agent Case Closing Responsibilities.
When completing investigations, ensure that the case file and the report are complete, accurate, and correctly assembled. SAs are responsible for preparing other forms, memoranda, and letters needed to supplement the report such as Form OI 2076, Form OI 2076-PDT, or cover letter to a prosecutor.

SAs are also responsible for making correct, timely and accurate entries into CRIMES, including required cross-indexing entries, as needed.

Note: ASACs are responsible for validating CRIMES information.

250.12 Referring Investigations to the IRS.
Any investigation that is of interest to the IRS, or where action by the IRS is required, whether it is an employee investigation or non-employee investigation, will be referred to the appropriate IRS office for action, or in some instances, for information only.

250.12.1 Referring Employee Investigations to the IRS for Action or Information. All employee investigations that were initiated based on a complaint will be referred to the IRS for administrative action where the subject is a named employee, or for information only where no specific IRS employee has been identified as the subject.

Generally, employee investigations that were initiated as spin-off cases from a TIGTA proactive investigative initiative but no wrongdoing by the subject employee was identified will not be referred to the IRS.

All referral of investigations to the IRS will be transmitted via Form OI 2076 or Form OI 2076-PDT. Ensure that all related cases are entered in Block 12 on the Form OI 2076.

250.12.1.2 Reports on IRS Employees. Reports on most IRS employees (regardless of grade level, position or violation) and lockbox and contract employees will be forwarded to:

Internal Revenue Service
1111 Constitution Avenue, NW
OS:HC:R:EC:EI:ROIU
NCFB - C1-530
Washington, DC 20224-0002

250.12.1.3 Reports on IRS Office of Chief Counsel Employees. Reports on IRS Office of Chief Counsel employees will be forwarded to:

Internal Revenue Service
Office of Chief Counsel
Deputy Chief Counsel
1111 Constitution Avenue NW, Room 3026
Washington, DC 20224

250.12.1.4 Reports on Enrolled Tax Practitioners. Reports on enrolled tax practitioners will be forwarded to IRS Employee Conduct and Compliance Office (ECCO) in Washington, DC. SAs will note in the Remarks section (Block 13) of the Form OI 2076 if the investigation involves a certified public accountant, attorney, or other enrolled tax practitioner and that the report should be forwarded to the Director, Office of Professional Responsibility.

250.12.1.5 Reports on Unenrolled Tax Preparers. Reports on unenrolled tax preparers will be forwarded to IRS ECCO in Washington, DC. SAs will note in the Remarks section (Block 13) of the Form OI 2076 that the investigation involves an unenrolled tax return preparer and that the report should be forwarded to SB/SE.

250.12.1.6 Reports on Assault/Threat/Interference Investigations. Reports relating to assault/threat/interference investigations will be forwarded on Form OI 2076-PDT to the IRS - Office of Employee Protection at the following address:

Internal Revenue Service
Office of Employee Protection
500 Woodward Avenue, Stop 30, Room 1238
Detroit, MI 48226

250.13 Distribution of Reports of Investigation to the IRS.
Distribute copies as follows:

- The SAC or ASAC, as appropriate, forwards a copy of the report and original Form OI 2076 or Form OI 2076-PDT to the centralized IRS office designated to receive the investigation.
- If the report was forwarded for action and response, the IRS will return to the SAC the Form OI 2076 or Form OI 2076-PDT, along with any documents from the IRS relating to the actions taken. Once the SAC updates CRIMES regarding actions taken, the Form OI 2076 or Form OI 2076-PDT will be associated with the case file and report.
- The IRS will not return its copy of the report to the SAC, but will destroy the report after it is no longer needed for an official purpose.

250.13.1 Distribution of Reports of Investigation in Theft and Embezzlement Cases.
At the completion of an investigation involving a theft or embezzlement, the SA will:

- Prepare a Form OI 2076 addressed to IRS ECCO and attach a copy of the report to the Form OI 2076; and
- Send the report with attached Form OI 2076 and a memorandum to the Director, Submission Processing Center, to IRS ECCO as instructed in this section. See Section 280.10.1 of this chapter for additional information on theft and embezzlement cases.

250.13.2 Authorization to Forward Cases to the IRS. Employee investigations that were initiated based on a complaint and where the subject is a named employee will be referred to the IRS for an administrative determination. Employee investigations being forwarded to the IRS for administrative adjudication will be approved and transmitted as follows:

- The ASAC will sign the Form OI 2028R as the approving official; and
- The SAC will sign the Form OI 2076; however, the SAC may delegate this to the ASAC.

Employee investigations where no specific IRS employee has been identified as the subject will be forwarded to the IRS for information only, and no response to TIGTA is required. These investigations will be approved and transmitted as follows:

- The ASAC will sign the Form OI 2028R as the approving official; and
- The SAC will sign the Form OI 2076; however, the SAC may delegate this to the ASAC.

Non-employee investigations being forwarded to the IRS for action or for information only will be approved and transmitted as follows:

- The ASAC will sign the Form OI 2028R, as the approving official; and
- The SAC will sign the Form OI 2076 or Form OI 2076-PDT; however, the SAC may delegate this to the ASAC.

250.13.3 Form OI 6441, Cover Sheet. Use Form OI 6441 as a cover sheet on all reports submitted to any function within IRS. The "Recommended Protection Level SP-3" means that the item must be stored in a locked container. Print Form OI 6441 on blue paper.

When transmitting reports to IRS facilities, SAs should use both an inner and outer envelope. The inner envelope should be marked "TO BE OPENED BY ADDRESSEE ONLY." Use a sealed mailbag or pouch as the outer wrapping.

Note: Place sexually explicit or other graphic material included in a report in a separate envelope that is clearly marked as to its contents and insert the envelope in the report where the material is referenced.

250.13.4 Employee Resignations. Even though the subject of an employee investigation may resign while under investigation, the report will be forwarded to the IRS as if the person were still on the IRS rolls. IRS will document ALERTS regarding the resignation.

250.13.5 TIGTA Employees. The SAC-IAD conducts investigations of TIGTA employees. Referral of these cases will be made in accordance with Section 330.7 of this chapter.

250.13.6 Referral Time Requirement. Refer investigations for administrative adjudication or information promptly, but no later than 45 calendar days after the last investigative step.

250.14 Referring Cases for Criminal Action.
SAs primarily investigate allegations of criminal violations of Titles 18 and 26 of the United States Code (U.S.C.) although investigation and prosecution of mission-related violations may require the use of other titles and statutes. SACs or their designees should consult with the U.S. Attorney to establish guidelines for:

- Referring cases for prosecution
- Interviewing subjects of investigation
- Establishing Blanket Declination Agreements (BDA)

Refer all cases to the local U.S. Attorney's Office or to the U.S. Department of Justice (DOJ) Tax Division when the investigation indicates that **a Federal law has been**

violated. SAs should document non-referrals in the Form OI 6501 and not in the Report of Investigation.

See Section 350 for referrals to DOJ-Tax.

See Section 280.13 regarding special procedures for criminal referrals involving substantive tax issues and financial crime-related employee misconduct.

250.14.1 Referral Time Requirement. Refer investigations for criminal prosecution promptly but no later than 45 calendar days after the last investigative step.

250.14.2 Formal Referral. A formal referral is the presentation of facts to an Assistant U.S. Attorney (AUSA) for a prosecutive or legal opinion. Formal referrals should be made in person if possible.

- Present the results of an investigation to determine if the AUSA will accept the case for prosecution;
- Prepare a Form OI 2028-M to document the formal referral of the case, including the AUSA's acceptance or declination, including their rationale for accepting or declining the case;
- Document declined formal referrals in the Report of Investigation;
- When declined cases involve grade 15 and above employees, request that the AUSA provide a written declination. If the AUSA will not provide a written declination, document this on Form OI 2028-M; and
- In block 12 of Form OI 2076, document the AUSA's acceptance or declination.

SAs must have the approval of an ASAC or higher-level manager prior to making a formal referral.

250.14.3 Informal Referral. An informal referral occurs when an SA contacts an AUSA prior to completing the investigation for prosecutive or legal opinions without disclosing the name or identifying information about the subject of the investigation. The SA presents general or hypothetical information about the case to determine if the AUSA is willing to prosecute that particular violation if facts develop which support the allegations.

Make an informal referral:

- During the early stages of an investigation;
- Before developing all the necessary elements of proof to sustain successful prosecutive action; and
- Prior to preparing the final report.

Prior to making an informal referral SAs must have the approval of an ASAC or higher-level manager.

- Prepare a Form OI 2028-M to document the formal referral of the case, including the AUSA's acceptance or declination, including their rationale for accepting or declining the case;
- Document declined informal referrals in the Report of Investigation; and
- In block 12 of Form OI 2076, document the AUSA's acceptance or declination.

NOTE: Do not document an informal referral in CRIMES as a referral and acceptance or declination. Absent a formal referral of the case to an AUSA, the case should be documented in CRIMES as "not referred."

250.14.4 Maintaining Liaison. When prosecutors defer opinions, maintain close liaison to avoid undue delays in decisions. Unnecessary delays may cause reversals of subsequent administrative disciplinary actions.

250.15 Blanket Declination Agreements.
A BDA is a written agreement between TIGTA and the incumbent U.S. Attorney. If a particular U.S. Attorney's Office advises it does not prosecute certain violations, include these violations in a BDA to prevent the need to refer these violations. The BDA states that the U.S. Attorney's Office will not prosecute cases that may be of a specific type, or have not met previously established criteria. SAs should:

- Document the Form OI 6501 with the specific statute declined pursuant to a BDA, the effective date of BDA, and the date the BDA was reviewed/applied;
- The preparation of a Form OI 2028-M to document the use of the BDA is not required;
- Select "Formal Written Blanket Declination" as the reason for the declined criminal referral and input the date the BDA was applied in CRIMES;
- Document the declination on the Report of Investigation synopsis with the following (or similar) general concluding statement, "Federal criminal prosecution of this case was declined by the United States Attorney's Office;" and
- In block 12 of the Form OI 2076, indicate that prosecution was declined.

250.15.1 SAC Responsibilities. The SAC shall maintain BDAs on file in the division.

BDAs will be confirmed at least every two years or:

- When events occur that might affect the status of the agreement; or
- When the President appoints a new U.S. Attorney.

When the BDA is confirmed, ensure that the BDA reflects the name of the current SAC of the division.

SACs will maintain written documentation of the biennial confirmation of the BDA (*e.g.*, a dated memo or email from the U.S. Attorney's Office) that identifies the applicable judicial district and the specific statute(s) or violation(s) that the BDA covers.

SACs will include scanned copies of all active BDAs in their respective divisions, including documentation of biennial confirmation, with the Case/Program Management SAC Certification.

250.16 Referrals to State/Local Authorities.
The TIGTA Chief Counsel's Office must approve all requests to refer information to State/local authorities for criminal prosecution prior to the referral. Before making referrals to State/local authorities consult Chapter 700, Section 70.5 of the TIGTA Operations Manual for the proper procedures.

250.16.1 Referring Assault Cases. If the AUSA declines prosecution of an assault case, discuss the option of referring the matter for State prosecutive consideration with the ASAC. Follow the procedures for referral as set forth in Chapter 700, Section 70.5.1.1, if the case is accepted for State prosecution

If the case is not referred for State prosecution or it is also declined by State prosecuting officials, interview the taxpayer and advise the taxpayer that:

- His/her actions may be a violation of law;
- No prosecution is pending; and
- Repeated acts may result in arrest, prosecution, and subsequent penalties.

In addition to the above, the SA should determine from appropriate questions asked, the subject's ability and determination to carry out the alleged threat.

Document in the report the results of the interview with the taxpayer. See Section 260.5 of this chapter.

250.17 Informal Discussions with Prosecutors.
SAs may conduct informal discussions with AUSAs or State/local prosecutors while developing investigations except investigations involving violations within the jurisdiction of DOJ-Tax. They do not need completed reports to hold these discussions. However, contact TIGTA Counsel prior to discussing matters with state/local prosecutors so as to avoid making an unauthorized disclosure. See Chapter 700, Section 70.5 of the TIGTA Operations Manual for the proper procedures.

250.18 Referring Civil Rights Violations.
The Assistant Attorney General, Civil Rights Division, established procedures for referring allegations of civil rights violations by IRS employees to the DOJ. The

procedures are contained in a memorandum, dated October 22, 1987, addressed to the Secretary of the Treasury. The memorandum directs, in part:

- When receiving information that an IRS employee may have committed a criminal civil rights violation, primarily 18 U.S.C. § 242, promptly report the allegations, by memorandum, to the Deputy Inspector General for Investigations (DIGI). The DIGI refers the matter to DOJ, Civil Rights Division.
- If the employee is the subject of a current investigation being conducted by OI, suspend the investigation.
- Resume the investigation after the DIGI receives approval from DOJ. This procedure prevents possible conflicts of TIGTA and DOJ objectives.

Prior to the DIGI referral, the Office of Chief Counsel should be consulted to review the information to identify potential disclosure issues or prohibitions. The disclosure restrictions may affect an FBI investigation into the matter.

After the Civil Rights Division officials review the matter, one of the following occurs:

- It is referred to the FBI for investigation; or
- It is returned to TIGTA for administrative disposition.

250.19 Reporting Results of Referrals.
Document the results of all referrals on Forms OI 2028-M and incorporate into the report. Include the following items regardless of whether the AUSA accepts or declines the case for prosecution:

- Date and place where facts were referred;
- Name and title of the AUSA or State/local prosecutor; and
- Prosecutive opinion, including the reasons for accepting or declining prosecution.

250.20 Providing Copies of Reports.
If the prosecutor wants a copy of the report before rendering an opinion or for additional information, forward a copy with a cover letter. The letter should state that the SA presented the case to the prosecutor and that the prosecutor requested further information. Enter all prosecutive decisions in CRIMES.

The SAC is the referral authority for reports being forwarded to an AUSA.

250.21 Cases Closed to File.
Cases closed to file involve investigations that are not referred for any administrative or prosecutive determination. The ASAC or higher level authority is authorized to close cases to file.

250.22 Program Weaknesses Identified During the Investigative Process.
The TIGTA-Office of Audit (OA) is responsible for conducting comprehensive, independent performance and financial audits of IRS programs and operations to, among other things, prevent, detect, and deter fraud, waste, and abuse. The Office of Inspections and Evaluations (I&E) conducts reviews, onsite inspections of offices, and in-depth evaluations of a major departmental functions, activities or programs.

Throughout the process of conducting TIGTA investigations, SAs will be alert to systemic weaknesses and vulnerabilities within IRS programs and operations that allowed the alleged wrongdoing or misconduct under investigation to occur.

When program weaknesses or questionable work practices create the climate for wrongdoing or misconduct, special agents will refer the investigative results through their SAC to OA or I&E for review and evaluation using the procedures below.

250.22.1 Referrals to OA. To refer a specific matter to OA, the SAC will prepare a memorandum through the Assistant Inspector General for Investigations (AIGI) to the appropriate Assistant Inspector General for Audit (AIGA). Memoranda to OA should include all of the following:

- OI case number (in the subject line or first sentence).
- Brief description of the investigative activity which prompted the referral.
- Statement of Problem(s) – Concise description of the program weakness or vulnerability identified by OI, to include location and scope.
- Details - Specific details on what was found and why an audit is warranted by OA. Whenever possible, recommendations to resolve the program weakness or vulnerability should be suggested.
- Point of contact information.

The AIGI, after concurring with the SAC's referral recommendation, will forward the signed memorandum to OA.

250.22.2 Referrals to I&E. To refer a specific matter to I&E, the SAC will prepare a memorandum through the AIGI to the Deputy Inspector General for Inspections and Evaluations (DIGIE). Memoranda to OIE should include all of the following:

- TIGTA-OI case number (in the subject line or first sentence).
- Brief description of the investigative activity which prompted the referral.
- Statement of Problem(s) – Concise description of the program weakness or vulnerability identified by OI, to include location and scope.
- Details - Specific details on what was found and why an inspection or evaluation is warranted by I&E. Whenever possible, recommendations to resolve the program weakness or vulnerability should be suggested.

- Point of contact information.

The AIGI, after concurring with the SAC's referral recommendation, will forward the signed memorandum to I&E.

250.23 Tax Audit Referrals to the IRS.
A tax audit referral by TIGTA differs from a regular audit examination only to the extent of TIGTA's interest in a related matter. In these examinations, the examiner performs the regular audit function in cooperation with TIGTA, but is not under the control or direction of TIGTA personnel.

For allegations of IRS employee tax fraud (*e.g.*, false returns), contact IRS CI, as detailed in the Memorandum of Understanding between IRS-Criminal Investigation and TIGTA. See Section 280.13.

250.23.1 Non-Employee Tax Audit Referrals to the IRS. Information developed by TIGTA or in the possession of TIGTA may have a bearing on the correctness of a tax return or on the determination of tax liability of a non-employee taxpayer. Refer information not obtained through a grand jury to the IRS for audit, where appropriate.

250.23.1.1 Non-Employee Tax Audit Referral Procedures. To refer a non-employee taxpayer to the IRS for audit, complete TIGTA Form OI 8109-NE, Referral for Examination of Non-Employee Income Tax Return. The form must be completed with all available information.

The SAC of the requesting division is the approval authority for non-employee tax audit referrals to the IRS.

Submit the approved form to the address identified in the form. The SAC will inform the AIGI, Cyber, Operations and Investigative Support Directorate, of any approved tax audit referrals.

250.24 Employee Tax Audit Requests.
To request a tax audit of an employee, complete TIGTA Form 8109, Request for Examination of Employee Income Tax Return Relating to a TIGTA Investigation.

Note: If closed years are involved, include sufficient basis to justify reopening of the closed years. See IRS policy statement P-4-3 and the Internal Revenue Manual (IRM). If the IRS official receiving a request for a tax audit determines that the examination is not warranted, the IRS will prepare a memorandum for the requesting SAC office that will explain the reason(s) the examination was not warranted.

The ASAC may contact IRS Exam Case Selection (ECS) Senior Program Analyst, as necessary, regarding the status of open requests, and the contact will be documented in

the case file. Contact the ASAC-Policy to identify the current IRS-ECS Senior Program Analyst.

250.24.1 Documenting Results of Employee Tax Audits. After receiving the examination report from the examiner, prepare a summary of the results on Form OI 2028-M and its effect upon the investigation or project. Include the summary in the investigative file.

250.25 Protection of Grand Jury Information.
There are no restrictions on the use of information or material presented to or developed by a grand jury after a court orders its unrestricted disclosure or the material is legally disclosed under another Federal Rule of Criminal Procedure.

Information supplied to the grand jury by OI from sources or leads independent of the grand jury process may be used for both the criminal purposes of the grand jury and the civil or administrative purposes of OI.

SAs must take special care to document sources of information and leads as OI may bear the burden of proving that evidence used for civil or administrative purposes was obtained independent of the grand jury.

SAs must ensure that any grand jury material is segregated from other case materials. They must:

- Index it as to the source of the material; and
- Ensure that only authorized persons review the material.

250.25.1 Dual Criminal and Administrative Investigations. There are instances where investigations have both criminal and administrative potential. It is imperative to separate grand jury material from other case material in these situations.

Prepare a detailed investigative work plan on Form OI 6501. Prepare a second Form OI 6501 to include all grand jury material as the circumstances dictate. If one lead identifies another lead, note the Forms OI 6501, with emphasis on dates of interview, identification of sources, etc.

At the time that an investigation is accepted for grand jury action, ensure that the Form OI 6501 is:

- Documented to sufficiently establish that all information and leads to that point were obtained independent of the grand jury;
- Expanded to include a comprehensive list of projected leads that would be pursued if the case were to be investigated as an administrative misconduct matter (in order to document that these leads were known prior to grand jury activity); and

- Documented to show that any information received independently of the grand jury, but after grand jury action has begun, has been received from a source not under grand jury process.

In situations where the subject enters a guilty plea, request that the USAO legally disclose in connection with the guilty plea as much grand jury material as possible for use in subsequent administrative proceedings.

250.25.2 Closing and Reporting Grand Jury Cases. At the conclusion of a grand jury investigation, return any material obtained by the grand jury process to the attorney for the Government. The attorney for the Government may instruct that the material be returned to the source. In preparing the report, be cautious in the writing of allegations, results of investigation, background information, details, and exhibit list sheet, so as not to disclose the specific content of the sealed pages.

Prepare and process reports containing grand jury information as follows:

- Type or stamp "Grand Jury Information" at the bottom of each Form OI 2028-M that contains grand jury information. Do not mark affidavits that contain grand jury information; treat them as listed below. Any question concerning whether information contained in the Form OI 2028-M is grand jury information should be discussed with the AUSA.
- Assemble the report and number the pages. After supervisory review, remove the pages and affidavits designated as grand jury information and replace them with blank pages entitled, "See Restricted File Envelope."
- Seal the removed pages and affidavits in a Restricted File Envelope affixed with TIGTA OI Form OI 6504 and insert the Form OI 6504 in the case file. List on the Form OI 6504 the names of authorized personnel who have access to the grand jury information. Only an authorized TIGTA employee can open the Restricted File Envelope; document each opening of the envelope in the space provided. Ensure that the pages in the Restricted File Envelope remain sealed until the information becomes public record or the court releases the information.
- Forms OI 6504 are maintained in accordance with Section 250.3.1 of this chapter.

DATE: October 1, 2020

CHAPTER 400 – INVESTIGATIONS

(400)-260 Assault/Threat/Interference Investigations and Armed Escorts

260.1 Overview.
The Office of Investigations (OI) investigates allegations of assaults, threats, or forcible interference against Internal Revenue Service (IRS) employees or contractors performing their official duties or activities otherwise intended to obstruct or impede tax administration. OI also provides physical security that includes providing armed escorts for IRS employees. This section contains the following information:

260.1.1 Acronyms Table.

260.2 Authority.
OI's authority to investigate threats, assaults, and related matters and to conduct armed escorts is derived from the Inspector General (IG) Act of 1978 and the Inspector General Reform Act of 2008 and is further described in Treasury Order 115-01. All reports of assaults, threats, or forcible interference against IRS employees performing their official duties must be provided to OI.

260.3 Jurisdiction.
Activities of groups, individuals, and individuals belonging to groups that advocate disruption of the Federal tax administration process and/or violence against IRS employees attempting to carry out their duties may come under the jurisdiction of multiple agencies, including:

- OI, because of OI's authority to investigate assaults or threats against IRS and contract employees and activities that are otherwise intended to impede tax administration; or
- IRS-Criminal Investigation (CI), because of willful failure to comply with the tax statutes.

For example, a threat, assault, or forcible interference could take place during a seizure of property by the IRS. IRS-CI has jurisdiction over forcible rescues of seized property in violation of Title 26, United States Code (U.S.C.) § 7212(b), but OI has concurrent jurisdiction over assaults and threats that occur in connection with forcible rescues. A determination of investigative interest will be made on a case-by-case basis in instances of overlapping jurisdiction.

See the Memorandum of Understanding Between IRS-CI and TIGTA-OI regarding investigative jurisdiction.

The Federal Bureau of Investigation (FBI) has concurrent jurisdiction over violence or threats of violence, including violations of the following:

- 18 U.S.C. § 241, 18 U.S.C. § 245, 18 U.S.C. § 1114, and 18 U.S.C. § 2383;
- The Civil Rights Act of 1968;
- Other related statutes; and
- Chapter 113B of Title 18, Terrorism. See also PDD-39, U.S. Policy on Counterterrorism.

260.4 Applicable Federal Statutes.
An assault, threat, or forcible interference against an IRS employee can be a violation of various Federal statutes but the most commonly used are:

- 26 U.S.C. § 7212(a), *Corrupt or forcible interference*; and
- 18 U.S.C. § 111, *Assaulting, resisting, or impeding certain officers or employees*.

Under 26 U.S.C. § 7212(a) and 18 U.S.C. § 111, if an IRS employee is threatened or assaulted based on the performance of their official duties, it is immaterial whether the act occurred during or after the employee's official duty hours.

260.4.1 26 U.S.C. § 7212(a). Unlike 18 U.S.C. § 111, 26 U.S.C. § 7212(a), *Corrupt or forcible interference*, includes threats of future harm and explicitly includes threats of bodily harm to any family member of an IRS employee. However, 26 U.S.C. § 7212(a) requires either the employee was acting in an official capacity under Title 26, or there was a connection to the due administration of the Internal Revenue laws. Additionally, as a result of U.S. Supreme Court decision, *Marinello v. U.S., 584 U.S. (2018)*, the Court held that in order for a conviction under § 7212(a), the following two standards

must be met: (1) there is a "nexus" between the defendant's conduct and a particular administrative proceeding, *e.g.,* investigation, audit, or other targeted administrative action, which requires a relationship in time, causation, or logic with the administrative proceeding; and (2) the defendant was aware of a pending tax-related proceeding, or that such a proceeding was reasonably foreseeable.

Further, "due administration" of the tax code refers to discrete, targeted administrative acts and does not cover every violation that interferes with routine administrative procedures, such as processing tax returns, receiving tax payments, or issuing tax refunds. Rather, the clause addresses specific interference with targeted governmental tax-related proceedings, *e.g.*, a particular investigation or audit. Additionally, a subject knowing that the IRS will review his or her tax return every year does not transform every violation of the Tax Code into an obstruction charge. A subject must know that the proceeding is at least in the near or foreseeable future, not just that the IRS may become aware of an unlawful scheme eventually.

Interference investigations involving violations of the "omnibus clause" of 26 U.S.C. 7212(a), such as non-forcible interference, must be referred to the Department of Justice Tax Division (DOJ Tax). See Section 350 for violations requiring referral to DOJ Tax.

260.4.2 18 U.S.C. § 111. Under 18 U.S.C. § 111, *Assaulting, resisting, or impeding certain officers or employees*, it must be established that assaults or threats of immediate harm were perpetrated while the IRS employee was engaged in the performance of official duties or on an account of official duties. Knowledge of the official capacity of the person assaulted is not necessarily required. For example, if an employee is threatened or assaulted while on official duty by an individual having no connection with any IRS activity, it would still constitute a violation under 18 U.S.C. § 111.

Violations of 18 U.S.C. § 111 must involve a threat of immediate harm. Threats of future force or harm alone are insufficient. The statute provides for an enhanced penalty of imprisonment for up to 20 years if a deadly or dangerous weapon is used or bodily injury is inflicted.

260.4.3 Additional Statutes. Additional Title 18 statutes to consider include:

- Section 372, *Conspiracy to impede or injure officer*;
- Section 875, *Interstate communications;*
- Section 1114, *Protection of officers and employees of the United States* (covers murder and attempted murder);
- Section 1501, *Assault on process server*;

- Section 1503, *Influencing or injuring officer, juror, or witness generally* (includes influencing, obstructing, or impeding the due administration of justice);
- Section 1505, *Obstruction of proceedings before departments, agencies, and committees* (includes the obstruction of investigations into tax returns);
- Section 1510, *Obstruction of criminal investigations* (includes acts of obstruction that are based on a reasonable belief a potential witness would pass information to investigators); and
- Section 2231, *Assault or resistance in searches and seizures*.

Title 18 U.S.C. §§ 1501 and 2231 concern assaults upon, resistance to, and interference with persons serving or executing legal process, or making searches and seizures.

260.5 Conducting an Assault/Threat/Interference Investigation.
Upon receiving a report of an assault, threat, or forcible interference against IRS employees in the performance of their duties, initiate an investigation in the Criminal Results Management System (CRIMES) using the appropriate violation code. Consider the following:

- Interview the assaulted or threatened employee as soon as possible after the incident is reported to OI;
- Advise IRS personnel not to contact the subject until OI's investigation is completed;
- Interview witnesses as soon as possible;
- Obtain a complete criminal history of the subject;
- Research CRIMES for any prior investigations on the subject;
- If conducting a tax administration investigation under Title 26, research IRS records (*e.g.*, Integrated Data Retrieval System (IDRS), CI records, etc.) for information on the subject;
- As warranted, attempt to secure a Form FOH-6, *Authorization for Disclosure of Information*, from the subject and request psychological support services from Federal Occupational Health (FOH). See Section 260.6; and
- Summarize in TIGTA Form OI 2028-M, *Memorandum of Interview or Activity*, any relevant information obtained from the medical/psychiatric files.

If the violation involves a physical assault or a threat of force or violence, obtain a prosecutive opinion from the U.S. Attorney's Office (USAO) and proceed with the investigation as directed by the USAO. See Section 350 of this Chapter for violations requiring referral to DOJ Tax.

At the conclusion of the investigation:

- Inform the assaulted or threatened employee of the final results of the

investigation as permitted by the Privacy Act and 26 U.S.C. § 6103;
- Complete TIGTA Form OI 8273, *Assault, Threat, Threat Assessment & Harassment Incident Report*, and include it as the first exhibit in the Report of Investigation (ROI);
- Refer the ROI to the IRS Office of Employee Protection (OEP) for a Potentially Dangerous Taxpayer (PDT) or Caution Upon Contact (CAU) determination; and
- Refer the investigation for prosecution as appropriate. See Section 260.7.

If the USAO declines prosecution, discuss the option of referring the matter for State or local prosecutive consideration.

- If a non-Title 26 investigation is conducted, discuss the case in general terms, absent identifiers or specific information about the case, with the State or local prosecuting authority to determine prosecutive parameters, without identifying the subject or specific facts of the case. See Chapter 700, Section 70.5.

260.6 Psychological Support Services.
Psychological support services are provided to OI by an FOH mental health professional. If the Special Agent (SA) believes that the subject of the assault/threat/interference investigation has a mental health condition, the SA may consult with the mental health professional to evaluate the subject's mental health and/or behavior. The purpose of this consultation is to assist the SA in articulating whether or not the subject may pose a danger to him/herself or others, or is capable of planning or carrying out an attack against the IRS or TIGTA personnel or assets. Not all assault/threat/interference investigations will warrant psychological support services. A mental health consultation should be requested when indicators of a possible mental health condition are present.

Before contacting the mental health professional, the SA should ask the subject:

- If he/she has a mental health condition;
- If he/she is currently being treated for a mental health condition or has been treated for a mental health condition in the past; and
- If he/she is on any medication.

The SA should attempt to obtain the subject's mental health/medical records by consent from the subject when practicable. Complete Form FOH-6 and obtain the subject's signature on the form. In some cases, mental health/medical records may be obtained by Inspector General subpoena or grand jury subpoena. FOH assistance will be based upon a review of medical records and other relevant material obtained by OI.

260.6.1 Requesting Psychological Support Services. Request mental health consultations through the Criminal Intelligence and Counterterrorism Division (CICD). CICD will coordinate the request with an FOH mental health professional.

The request should be made in writing (*e.g.*, e-mail) by the SA through his/her Assistant Special Agent in Charge (ASAC) to the CICD Assistant Director (AD)/ASAC. Include in the subject line of the e-mail, "Psychological Support Services Request," and provide the case number and case name in the subject line. For example, *Psychological Support Services Request: 55-XXXX-XXXX-I Doe, John*.

The written request should:

- Describe the allegation/investigation;
- Summarize the subject's mental health/medical history;
- Provide a justification for the mental health consultation request (*i.e.*, why do you need the subject's mental health/medical records?); and
- Indicate the urgency of the request (*i.e.*, how soon do you need the consultation completed?)

CICD will notify the mental health professional that a request for services has been made and will provide him/her with the requesting SA's contact information. The mental health professional will contact the SA upon receipt of the request. The mental health professional will review the mental health/medical records of the subject and provide the SA with a mental health assessment of the subject.

Notify CICD via e-mail when the mental health consultation is completed.

260.6.2 Storing Mental Health/Medical Records. Maintain all mental health/medical records in a Restricted Folder. The folder should be marked "medical confidential."

260.7 Report of Investigation.
Prepare ROIs in accordance with Section 250.7 of this chapter. The report must include:

- TIGTA Form OI 8273 as the first exhibit; and
- TIGTA Form OI 2028-M documenting the subject interview, if conducted.

Refer the investigation to the IRS as appropriate. See Section 250.12.

Note: Information from TECS or other criminal history information databases (*e.g.*, National Crime Information Center [NCIC]) must be verified through the originating agency. Information that has not been verified with the source cannot be included in the ROI or disseminated outside of TIGTA. See Section 150.4.3.

260.7.1 Referral for PDT/CAU Determination. When an investigation is initiated on a named subject using violation code 155 (5 Year Update) in CRIMES, IRS-OEP is notified automatically by means of an electronic interface between CRIMES and the PDT database. IRS-OEP then takes preliminary steps to designate the subject as a

pending PDT, if appropriate. The interface with IRS-OEP does not apply to violation codes 151-Armed Escort and 161-Workplace Violence.

When the investigation is completed, the Special Agent in Charge (SAC)/Director or his/her delegate will refer the ROI to IRS-OEP for a final PDT/CAU determination. See Section 250.12 of this chapter for referring an assault or threat investigation to the IRS.

Note: If the investigation has been accepted for prosecution, discuss with the ASAC/AD whether the referral to IRS-OEP should be delayed pending the outcome of any legal action so that IRS-OEP can be provided with the complete results of all investigative and prosecutorial activities for its consideration.

The referral and determination are required even in those instances where the subject is already designated as a PDT/CAU.

260.8 Referral for Prosecution.
Refer assault/threat/interference investigations for prosecution.

260.8.1 Referral to the United States Attorney's Office. Refer criminal violations to the USAO as described in Section 250.14 of this chapter. If the USAO declines prosecution, discuss the option of referring the matter to State or local authorities for prosecutive consideration.

260.8.2 Referral for State/Local Prosecution. If there is State or local prosecutive interest, refer the ROI through the Office of Chief Counsel to the relevant State or local court prosecuting authority. Follow the referral procedures set forth in Chapter 700, Section 70.5.

For investigations involving violations of Title 26, the entire investigation is the return information of the subject of the investigation and is protected in its entirety from disclosure by I.R.C. § 6103. The SA must obtain consent from the subject of the investigation before having any discussions, including discussions in general terms, absent identifiers or specific information about the case, with the State/local prosecutor regarding the investigation and/or referring the investigation to the State/local prosecutor. See Chapter 700, Section 70.5.

260.8.3 Arrests in Assault/Threat/Interference Investigations. Whenever possible, contact the USAO or an appropriate person at DOJ before making an arrest. In exigent circumstances, a felony arrest in an assault, threat, or forcible interference investigation may be made without a warrant and without conferring with the USAO or official of the DOJ. See Section 140.

A misdemeanor arrest in an assault, threat, or forcible interference investigation may not be made without the issuance of an arrest warrant, unless the misdemeanor occurs in the arresting SA's presence.

SAs are not authorized to execute State/local arrest warrants on investigations referred to and accepted by State or local prosecutors.

Coordinate with the TIGTA Public Affairs Liaison and the USAO or other responsible DOJ officials to assure appropriate publicity of the arrest.

260.9 PDT Program.
The IRS established the PDT program in 1984 to improve the IRS's ability to identify taxpayers who present a potential danger to employees attempting to do their jobs. The IRS-OEP administers the program. See Internal Revenue Manual (IRM) 25.4.1 for information on the PDT program.

260.9.1 OI PDT Responsibilities. OI is responsible for the following:

- Conducting investigations of alleged assaults, threats, interference, or potential threats against IRS and contract employees; and
- Referring ROIs relating to alleged assaults, threats, interference, or potential threats to the IRS-OEP for a PDT determination.

260.9.2 IRS-OEP PDT Responsibilities. IRS-OEP is responsible for the overall operation, management, and oversight of the PDT program. These responsibilities include the following:

- Making PDT determinations in conjunction with appropriate IRS management officials;
- Inputting PDT designations into the IRS Master File;
- Removing PDT designations from the IRS Master File;
- Maintaining a computerized file of background information on each PDT; and
- Reevaluating the status of PDTs every five years.

260.9.3 PDT Criteria. A PDT designation must be based on verifiable evidence or information that is relevant to tax administration. Taxpayers must be identified by Social Security Number (SSN) and/or Employer Identification Number (EIN). Association with a PDT or membership in a group whose members advocate violent protest against the tax system does not by itself necessarily fulfill the criteria for designation as a PDT.

The IRS Commissioner and Chief Counsel approved the following criteria for determining PDT status:

- Individuals who, within the past 10 years, have physically assaulted an IRS employee, a former employee, a contractor, or an immediate family member of an IRS employee, a former IRS employee or a IRS contractor;
- Individuals who, within the past 10 years, have intimidated or threatened an IRS employee, a former employee, a contractor, or an immediate family member of an IRS employee, a former employee, or a contractor through specific threats of bodily harm, a show of weapons, the use of animals, or through specific threatening behavior (*e.g.,* stalking);;
- Individuals who, within the past 10 years, have advocated violence against IRS employees where advocating such violence could reasonable be understood to threaten the safety of IRS employees and/or impede the performance of IRS duties;
- Individuals who, within the past 10 years, have been members of, or affiliated with groups that advocate violence against IRS employees, where advocating such violence could reasonably be understood to threaten the safety of IRS employees or impede the performance of IRS duties;
- Individuals who, within the past 10 years, have committed the acts set forth in any of the preceding criteria, but whose acts have been directed against employees or contractors of other governmental agencies; or
- Individuals who are not classified as PDTs through application of the above criteria, but whose acts within the past 10 years have demonstrated a propensity for violence.

260.9.4 PDT Designation When No Overt Threat/Assault. An employee who obtains information that does not involve an overt threat or assault but indicates that a group or individual may pose a threat to IRS employees' safety should report this information through IRS management to OI. OI may also identify such groups or individuals through its own investigative initiatives.

For IRS-OEP to make a valid PDT determination on individuals in these situations, there must be documentation of the specific activities of the group or individual indicating a propensity towards violence that leads to the conclusion that individual members of the group pose a threat to the safety of IRS employees.

If a general characterization of a taxpayer such as “known to be violent” is used in the ROI, the statement must be based on specific overt actions by the subject or on statements given by witnesses. Document in the ROI any such overt act or statement. If the names of members of a violence prone group are reported, list the basis for knowledge of membership. See Section 410 of this Chapter. See Section 260.12.1

regarding the inclusion of sensitive information (*i.e.,* classified or not approved for dissemination by originating agency).
RRA 98 prohibits the IRS from designating taxpayers as "illegal tax protesters" or any similar designation; therefore, such terminology should not be used.

260.9.5 Suicide Threats. A PDT determination may be justified if the suicide threat states or implies harm to an IRS or contract employee or the IRS or contract employee's immediate family.

260.9.6 IRS Records Displaying PDT Indicator. IRS employees are alerted that a taxpayer has been designated as potentially dangerous by symbol "*PDT*" being prominently displayed on the taxpayer's IDRS account and all documents originating from IDRS.

When the PDT indicator is input into IDRS, the indicator posts to the Master File. The indicator remains on IDRS as long as the PDT indicator is present on the Master File.

See 260.11 and 260.14 of this section for additional information on personal contacts with PDTs and armed escort requests.

260.9.7 Five Year PDT Updates. Five years after a PDT designation has been made, OI conducts a follow-up assessment of the taxpayer so a new determination can be made. Five-year updates are processed as follows:

- OEP provides a list of PDTs to CICD;
- CICD compiles the basic identifying information, initiates an intake in CRIMES, and transfers the complaint to the appropriate field division;
- Field divisions initiate an investigation using violation code 155-5 Year Update, and, at a minimum, conduct the following investigative steps:
    - Conduct criminal history research;
    - Verify and obtain any additional information related to criminal history research; and
    - If appropriate, request an Intelligence Analyst Report (IAR).

The ROI should be referred to OEP before the PDT expiration date.

The ROI does not need to include TIGTA Form OI 8273, a subject interview, or prosecutive opinion from the USAO or State/local prosecutor's office.

260.10 CAU Program.
The CAU program was established after the passing of the IRS Restructuring and Reform Act of 1998 (RRA 98) to capture those taxpayers whose behavior did not meet PDT criteria, but who still required a more cautious approach by IRS employees. The

program captures those taxpayers who have threatened to commit suicide or threatened to file frivolous liens or lawsuits against IRS employees. See IRM 25.4.2 for information on the CAU program.

260.10.1 OI CAU Responsibilities. OI is responsible for the following:

- Conducting investigations of alleged assaults, threats, or interference against IRS and contract employees and suicide threats, as warranted; and
- Referring ROIs relating to alleged assaults, threats, interference, and suicide threats to IRS-OEP for a CAU determination.

260.10.2 IRS-OEP CAU Responsibilities. IRS-OEP is responsible for the overall operation, management, and oversight of the CAU program. These responsibilities include the following:

- Making CAU determinations in conjunction with appropriate IRS management officials;
- Inputting CAU designations **** *** *** ****** ****;
- Removing CAU designations from the *** ****** ****;
- Maintaining a ********** **** ** ********** ********** ** **** ***; and
- Reevaluating the status of CAUs every five years.

260.10.3 CAU Criteria. The designation of a CAU must be based on reliable evidence or information. There must also be a nexus to tax administration. Taxpayers must be identified by SSN and/or EIN. Taxpayers who have been identified as PDTs cannot also be designated on IDRS/Master File as a CAU, as the PDT designation takes precedence over the CAU designation.

IRS Chief Counsel has determined that a suicide threat is not, in itself, sufficient justification for IRS-OEP to designate an individual as a PDT. However, it may be sufficient justification for IRS-OEP to designate an individual as a CAU.

The following criteria have been established for determining CAU status:

- Specific information has been developed to suggest a subject's actions could pose a threat to the IRS or IRS employees, but the information is restricted and cannot be released and included into the ROI because it is either classified for national security reasons or the originating agency has restricted its dissemination. See Section 260.12.1;
- Individuals who, within the past 10 years, have threatened physical harm that is less severe or immediate than necessary to satisfy PDT criteria;
- Individuals who, within the past 10 years, have threatened suicide; or
- Individuals who, within the past 10 years, have filed or threatened to file a frivolous lien or a frivolous criminal or civil action against an IRS employee, a

former IRS employee, a IRS contractor, or an immediate family member of an IRS employee, a former IRS employee, or a IRS contractor.

260.10.4 IRS Records Displaying CAU Indicator. IRS employees are alerted that a taxpayer should be treated with caution upon contact by the letters "CAU" being prominently displayed on the records and databases listed in Section 260.9.6.

260.11 Contact with a PDT or CAU.
If a taxpayer makes an inquiry about his/her PDT or CAU status, do not confirm or deny that the taxpayer is a PDT or CAU. Refer the taxpayer's request to the local IRS Disclosure office.

260.11.1 Office Visit by a PDT. If an IRS employee learns a PDT will visit an IRS office, or if the PDT is in the IRS office, the employee's manager may contact the nearest TIGTA office to request an armed escort. The assigned SA, the IRS manager, and the IRS employee will evaluate the situation and determine the following:

- Should the office interview be held?
- Who will attend the interview, if held?
- Will the SA be present at the interview, be on stand-by during the interview, or meet with the taxpayer at the office prior to the interview?
- Will the SA introduce him/herself to the taxpayer and advise the taxpayer that he/she is there for the safety of the IRS employee?
- Will the SA ask the taxpayer if he/she is armed and any other safety-related questions?

If TIGTA cannot provide the armed escort, coordinate the armed escort with the nearest IRS-CI office.

260.12 Threat Assessments.
Both IRS-CI and OI maintain a liaison with the FBI concerning the activities of groups that advocate the disruption of the Federal tax administration process and/or violence against IRS employees. OI has a headquarters liaison with FBI headquarters to ensure coordination between the FBI and OI. This liaison ensures the following:

- A coordinated effort exists between IRS-CI and OI, limiting each agency to matters within its respective jurisdiction;
- Duplication of investigative effort is eliminated; and
- Both parties facilitate the timely exchange of information authorized for release.

OI and IRS-CI are authorized to solicit and receive information concerning groups or individuals involved in efforts to disrupt Federal tax administration, or situations

involving potential assaults or threats against IRS or contract employees. Information on other matters relating to these groups should be referred to the FBI.

When OI receives names of potentially dangerous taxpayers from another source, OI will conduct an investigation to independently verify that the taxpayers will likely meet the PDT/CAU criteria before forwarding an ROI to IRS-OEP for a PDT/CAU determination.

260.12.1 ********* ****** ******** ******** **********. **** ********* ********* ** ******** ****
****** *** *********** ****** ********** ** ********** *** *** * ****** ** *** *** ** *** *********. ***
*** *********** ****** ** ****** ********* ******* *** ********** *** **** ********** *** *******
******** ******* ** *** *********** ******* *** ********** *** ********** *** ******** *********
****** ** ********** ** *** *** ******** ********. "***** ********** *** ******** **********
********* **** ******** **** *** ******'* ******* ***** **** * ****** ** *** *** ** *** *********. ***
******* ****** ** ********** **** *******. ******** *********** ** *** ******** ** *** ****** ******* **
** ****** ********* *** ******** ******** ******* ** *** *********** ****** *** ********** ***
**********."

******** ** **** *** ***** ********* ***** ** **** ******* **** ********** ***/** ********* **********
** ******** **** ** *** ******* ********* ** **** ******* ******'* ******* **********, *********
************ ******** ******* ** ** ***** ********** **** ***** *** *** *********** ****** ***
********* ********** *** ******* ************ ** ** ********* ** ******* *** ******** ** ***
**********. **** ***** ********** *****, *** ** ***** **** ** ******* ** ***** *** ********** *******
*** ********** ****** ** ****** *** ******* ********** ** ***** ********** ** ** * ****** ****** *** ***
** *** *********.

*** ** **** ********* *** ****** ** *** ********* ** * ***** **** ** ****-*, ********* ** ******** **
********, ** ********* *** *********.

- ***** *** ********** *** *******;
- **** ** *** ********. ***
- *** *********** ******** *** ******* ** * ****** ** *** ** *** *********, *** *** ************
  ****** *** ********* *** ************* *******.

*** ***** **** ** ****-* **** ** ******** ** ** ******* ****** *** ***. *** **********.** * *, *********
*** *********** ** ***** **** **** ***** ************ *** *******. ********** *** ***** ***** *********
****** ** ********** ** * ***** **** ** ****-* *** ** *** *************** ***** ***/** **** ** *
************** ********* ******, **** ****** ** ********* ********* *** ********** **********.

****. *** ***** ********* **** *** ***** ** ******* ****** ******* **** ** ***** ** ****** ******* **
***** ****** **** *** ********* *** *** ********** *** ****. *** *********** ********* ** *********
*********, **** ** *********** **** ********* *** ********* ****** ** ********* ***, ******** ********, *

***** **** ** ****-* ***** ** ******** ** ******** *** ********* *** ********** *********** ** **
******* ** *** ***, ** **********.

260.12.1.1 CICD Notification. ASACs will notify CICD by e-mail (*TIGTA Inv CICD Criminal Intelligence) of all cases where the potential threat involving Restricted Information statement will be used. Notification should be made as soon as the information is received indicating an individual is a potential threat toward the IRS or IRS employees, but the originating agency has restricted further dissemination of the information. Upon notification, CICD will contact the assigned SA to provide assistance and will coordinate with the Federal agency holding the information and OEP, as appropriate.

See Chapter 700, Chief Counsel, Section 50 of the TIGTA Operations Manual concerning questions related to disclosure issues.

260.12.2 Groups of Interest. See Section 410.5.2 for information concerning investigations into the activities of anti-tax or anti-government groups or individuals who promote violence against the IRS and its employees.

260.12.3 Other Threats. All threats to IRS-occupied buildings involving the use of explosives, incendiary, chemical, or biological devices should be documented and reviewed and, if appropriate, investigated. These threats may have significant potential for harming or intimidating IRS employees and property, as well as interrupting the effective administration and enforcement of tax laws.

260.13 IRS Protection.
IRS-CI is responsible for providing protection to the IRS Commissioner.

OI will:

- Respond to emergencies involving the physical safety of IRS employees, contractors, and facilities and will take action consistent with the agency's jurisdiction, but will not provide routine security services, such as screening persons accessing IRS facilities. IRS-CI or local law enforcement, as appropriate, will respond to emergencies if no TIGTA personnel are on-site.
- Provide armed escorts for IRS employees, informants, and witnesses, and other eligible persons, as warranted. Armed escorts will be provided at OI's discretion on a case-by-case basis. OI has the sole authority and responsibility for providing armed escorts. See Section 260.14 for additional information regarding armed escort requests.
- Investigate assaults and threats per Sections 260.5 and 260.13.2, including those that occur during a forcible rescue of IRS property.

260.13.1 Additional Protection. Situations may arise when it is necessary to provide additional protection to an IRS or contract employee and his/her immediate family. When an IRS or contract employee receives information alleging a threat or possible danger to a past or present IRS or contract employee, confidential source, witness, or the family or close associate of the IRS or contract employee, the appropriate Assistant (AIGI) or Deputy AIGI will determine if providing protection during regular and off-duty hours is necessary and appropriate.

See Sections 230.9 and 230.10 of this chapter for information on protection of victims and witnesses.

260.13.2 Forcible Rescue Investigations. Assaults and threats to IRS employees during forcible rescues are within TIGTA's jurisdiction and are addressed in Section 260.2. However, IRS-CI has the investigative responsibility for forcible rescues of property from the IRS in violation of 26 U.S.C. § 7212(b). If an assault or threat occurs in the course of a matter pending before IRS-CI (*e.g.,* search warrant, arrest), IRS-CI may take appropriate enforcement action to ensure the safety of those involved. IRS-CI will promptly notify OI and provide documentation concerning the incident and action taken.

For additional information regarding investigative jurisdiction, see the Memorandum of Understanding Between IRS-CI and OI.

260.14 Armed Escorts.
On October 14, 2008, the President signed Public Law 110-409, Inspector General Reform Act of 2008, which lifted the statutory prohibition against TIGTA providing physical security to protect the IRS against external attempts to threaten IRS employees. This statutory revision allows TIGTA to conduct armed escorts to protect IRS employees. On May 2, 2011, in accordance with an agreement between OI and the IRS, OI assumed the responsibilities related to all armed escorts. OI may provide armed escorts to IRS personnel, IRS contractors, informants, witnesses, and other eligible persons when warranted.

260.14.1 Armed Escort Requests. The request for an armed escort will be made via memorandum from the IRS employee's supervisor to the SAC of the division where the escort is needed. To ensure the safety of all personnel involved, requests should be submitted at least one week prior to the scheduled activity. If a request is submitted less than one week from the scheduled activity, postponement of the activity may be necessary.

Upon receipt of a request for an armed escort, initiate an intake in CRIMES using the violation code 151-Armed Escort unless OI already has an open investigation on the subject (*e.g.*, an ongoing threat investigation). Once the ASAC/SAC has approved the armed escort, initiate an investigation.

When there are multiple requests for an armed escort, initiate a new armed escort intake/investigation whenever a new operational plan is prepared.

If OI provides an armed escort on an open investigation with another violation code, ensure CRIMES violation code 151-Armed Escort is added to the violation profile and the circumstances are documented in the "Results of Investigation" section of the investigation screen.

260.14.2 Armed Escort Approvals. All armed escort requests will be reviewed by the respective SAC and will be approved on a case-by-case basis. The SAC can delegate this authority to the responsible ASAC as appropriate. If the approving authority determines that an armed escort is not warranted, IRS management may seek a reconsideration of the denied request by contacting the respective SAC. If the SAC denies the request and the IRS management official still believes an armed escort is warranted, the IRS management official can request a final reconsideration from the appropriate AIGI or Deputy Assistant Inspector General for Investigations-Field Operations.

In accordance with an agreement between OI and the IRS, IRS management may not request and/or alternately seek assistance from IRS-CI if their request for an armed escort has been denied by TIGTA. If IRS-CI receives a request for an armed escort from an employee/management official, IRS-CI will refer the employee/management official to the nearest OI office.

260.14.3 Planning the Armed Escort. The objective of an armed escort is to ensure the physical safety of all involved. Proper planning of the operation will reduce the possibility of injury to any individual.

When planning an armed escort:

- Review the armed escort request from the IRS employee/supervisor.
- Interview the IRS employee and his/her supervisor regarding the taxpayer, planned date, time, and location of the armed escort.
- Consider the following issues:
    - During any previous contact did the taxpayer verbally or through body language pose a threat?
    - What prior audit or collection action was taken against the taxpayer?
    - Does the IRS employee know of any weapons that the taxpayer might have at the contact location?
    - Obtain the physical description of the taxpayer from the IRS employee.

- Obtain a description of the contact location. If the planned contact is in an IRS office, survey it for potential weapons such as scissors, letter openers, staplers, etc.
- If contact is at the taxpayer's business, ascertain the type of business and its normal operating hours. Are employees, family, and/or customers likely to be present at the location?
- Time of contact - The IRS employee will usually want to contact the taxpayer at a time when maximum assets are available. If this creates a safety problem, the SA should point this out to the IRS employee and suggest he/she contact the taxpayer at a time more conducive to safety.
- What are the minimum IRS tasks the employee must conduct in order to carry out his/her responsibilities?

- Advise the IRS employee and his/her supervisor of the role of TIGTA SAs and discuss the expected role of the IRS employee.

260.14.3.1 TIGTA vs. IRS Responsibilities During Armed Escort. OI's primary responsibility during an armed escort is to protect IRS employees and other individuals present to effectuate the IRS activity. Any other law enforcement activity, such as arresting the taxpayer and/or seizing evidence, is secondary to OI's responsibility to provide physical security for the IRS employee.

The IRS employee is responsible for all IRS business-related details.

260.14.3.2 ********** *******. *** ** ****** ******* ***** ** ***** *** ******** ********** ****** ** ** ***** ******. ** ********* ******* ******/********* ******** *** ********.

- ****;
- *****;
- ********** ********** ********** ******;
- ********** ** ***** ******* *****;
- ***** ****** ******* ****** ***** ********; ***
- **** ***.

********* ******** *** ***********:

- ***** ****** ******** (** *** ****** ** *** ** ****** **** ***** *** **********, ** **/*** "******" ** ****?);
- ***** *** ****** ** ******* ** ********** ******** ** ********** *** ******** (*.*., ***'* ******** ********** ********* ******);
- ****** ** *******, *******, ******** *** **********;
- ******* ***** ******* ** ********** (*.*., ********* ** ******* ********, ***.);
- ********* ******* (*.*., **********, *****, **********); ***

- ***** *** ***** ****** ******** *** ***** ******* (*********'* ****** ******* *** ********* *********, ** **********).

260.14.3.3 Protective Vests. The SA should contact the National Firearms, Agent Safety, and Tactics (FAST) Coordinator to request protective vests for the escorted employees, as warranted.

260.14.3.4 Assistant United States Attorney Contact. The SA should discuss arrest authority and parameters with an Assistant United States Attorney (AUSA) regarding actions in the event the taxpayer physically assaults or threatens IRS/TIGTA personnel, offers passive resistance during the operation, is armed, or has access to a weapon. See Section 140.4.2 regarding arrests.

260.14.3.5 Operational Plan. The SA must complete TIGTA Form OI 7504, *Operational Plan for Armed Escort, Surveillance, Undercover, and Arrest*.

Consider the following:

- Local police notification or assistance, if appropriate;
- If OI requires the assistance of IRS-CI for the armed escort, the OI SAC will forward a request in writing to the appropriate IRS-CI Director Field Operations (DFO) for concurrence. Upon approval from the DFO, OI will coordinate with their local IRS-CI office. OI will be responsible for the risk assessment and all administrative requirements associated with the IRS armed escort program;
- Protective vests (SAs must make body armor available to IRS employee(s) if requested);
- Shotgun/AR-15 (See Section 130.8.3.2 for deployment criteria);
- Location of the IRS employee;
- Number of expected IRS employees/agents/taxpayers;
- Observation/surveillance of location, if applicable;
- Communications equipment;
- Location of appropriate U.S. Magistrate and jail facilities;
- Transporting prisoner in the event of an arrest;
- Writ of Entry limitations (what areas of the property are included/excluded?);
- Identity of known associates and family members (are they threats, are they likely to be present?); and
- Identify any groups/organizations to which the taxpayer belongs that advocate violence towards Government employees.

Ensure TIGTA Form OI 6501, *Chronological Case Worksheet* is documented to reflect pre and post-operational briefings, in addition to all operational activities. See Section 250.4.3.

The ASAC must review and approve TIGTA Form OI 7504.

260.14.3.6 Pre-Operational Activity. When possible, conduct a pre-briefing with all TIGTA/IRS personnel involved in the armed escort prior to the armed escort. The briefing should include information about the following:

- Subject taxpayer;
- Planned IRS activity;
- Possible weapons owned by the taxpayer;
- Any security concerns; and
- Each person's roles and responsibilities.

The SA should advise the IRS employee that TIGTA SAs will make the initial contact with the taxpayer and control the situation before the employee is introduced. Safety is OI's primary concern.

The SA should ensure that the responsible IRS employee has the necessary paperwork and sufficient personnel to accomplish seizing, inventorying, loading, and moving the assets. This will help ensure the operation's completion without unnecessary delay and with minimum risk.

The SA may abort the operation if circumstances cause him/her to determine that continuing the operation will pose a danger to TIGTA or IRS personnel.

If possible, the SA should conduct an advance surveillance of the location just before the armed escort operation begins to observe and report changes from the pre-operational surveillance and other factors that the SAs have no influence/control over. The SA should consider having another SA on static surveillance of the location, if possible, to report information to the team at the staging area.

260.14.4 Conducting the Armed Escort. Upon arrival at the armed escort location, SAs will secure and control the situation before the IRS employee and taxpayer meet. Allow the employee to approach the taxpayer only if it is safe. As warranted, before allowing the IRS employee to contact the taxpayer, SAs should:

- Approach the taxpayer and identify themselves.
- Confirm the identity of the taxpayer.
- State the purpose of the SAs' presence.
- Ask the taxpayer if he/she is armed.
- Visually survey the area for weapons or any items that could be used as weapons.
- Secure any weapons as appropriate with the taxpayer's consent, or consider moving to another area if weapons are available.

- Introduce the IRS employee when appropriate.

The SA cannot require the taxpayer to leave the location or remain in one specified area during the armed escort unless a crime is/has been committed and an arrest is warranted. If the taxpayer is not cooperative, the SA should articulate his/her responsibility to balance the aspects of officer safety, IRS employee safety, and the taxpayer's freedom of movement. Remain vigilant and maintain visual surveillance of the taxpayer as much as possible.

If illegal items or contraband are observed in plain view, take appropriate steps to notify appropriate law enforcement agencies, as warranted. Once the IRS employee has conducted the necessary IRS activity, leave the location immediately. Do not stay on-site to discuss the armed escort operation. Prior to leaving the armed escort location, ensure all IRS/TIGTA personnel and equipment are accounted for.

260.14.4.1 Use of Force. Only use force that is reasonable and necessary to protect the employee in the performance of his/her duties. An IRS employee is not authorized to use force in the seizure of property. An IRS employee must also have either written consent from the rightful owner or a Writ of Entry (court order) to enter the private areas of personal or business premises of a taxpayer. A Writ of Entry authorizes the IRS employee to enter the premises and seize property to satisfy a tax liability; it is not a search warrant. See IRM 5.10.2.16.3 and 5.10.3 for IRS policy and procedures on consent and Writ of Entry.

If a taxpayer uses passive resistance in an attempt to impede the IRS activity, advise the taxpayer of a possible violation of Federal statute [*e.g.,* 26 U.S.C. § 7212(a)]. If the taxpayer continues passive resistance and an on the spot arrest is not justified, withdraw from the situation and report the details of the incident to the AUSA, ASAC, and IRS employee's manager, if applicable.

- Examples of passive resistance:
  - The taxpayer blocks or holds onto the doorway preventing entry;
  - The taxpayer physically holds onto assets preventing the seizure;
  - The taxpayer locks him/herself inside the asset, preventing the seizure.
- If third parties attempt to intervene, advise them that they are violating Federal law 26 U.S.C. § 7212(a) by interfering; or
- If sufficient personnel are not available to control the situation, withdraw from the site. TIGTA's purpose for being there is to protect the employee.

Exceptions to withdrawing from the situation include the following:

- If the taxpayer physically assaults an IRS employee or anyone acting as an agent (*e.g.*, tow truck operator, locksmith, local police, etc.), the taxpayer should

be arrested for a violation of 18 U.S.C. § 111. However, the arrest is secondary to the IRS employee/contractor's safety. See Section 140.4 of this Chapter for more information on arrests;
- The taxpayer makes a verbal threat and the AUSA has previously authorized an arrest; or
- Other situations previously authorized by the AUSA.

260.14.5 Post-Operation Procedures. Conduct a post-operation briefing regarding the armed escort with the IRS employee and his/her supervisor. Conduct a separate post-operation briefing with TIGTA personnel.

Update CRIMES to reflect the appropriate armed escort information.

260.15 Employee Pseudonyms.
When an IRS employee who uses a registered pseudonym is the subject of a TIGTA investigation or complaint, or provides information to TIGTA in any capacity, document the employee's true identity in CRIMES and throughout investigative reports. The purpose of a pseudonym is to provide a layer of protection for the employee from taxpayers that may pose a threat to employee's personal safety. To maintain the integrity of the employee's pseudonym, the pseudonym should be used and referenced when speaking with the subject(s) and witnesses during an investigation.

See the IRS's Internal Revenue Manual, Section 10.5.7.1 for information concerning the use of pseudonyms by IRS employees.

260.16 Workplace Violence.
OI has primary jurisdiction for investigating the misconduct aspects of workplace violence or threats of workplace violence. If a personal dispute between employees results in potential danger to other employees in the workplace, OI may intervene for employee safety.

OI investigates employees who harass, intimidate, threaten, and/or assault their fellow employees. After assessing such misconduct, OI may:

- Initiate an employee investigation;
- Report the situation to State or local law enforcement authorities; or
- Refer the matter back to management for administrative action.

Workplace violence issues can generally be categorized as follows:

- Imminent danger or physical assault;
- Verbal threats of bodily harm reported, but no ongoing activity; and

- Inappropriate statements/behavior.

The first two categories require OI involvement at some level, or other law enforcement involvement if the situation so dictates. The third category should initially be addressed by management (*i.e.*, TIGTA management if a TIGTA employee is involved or IRS management if an IRS employee is involved) when there are no threats of bodily harm.

260.16.1 Response to Workplace Violence and Threatening Situations. An immediate law enforcement response is necessary in the following workplace violence situations:

- A physical assault causing harm or serious bodily injury; or
- A credible threat of imminent harm or serious bodily injury.

IRS/TIGTA should promptly notify OI of these situations; however, the following should be considered for incidents requiring an immediate law enforcement response:

If...	**Then...**
OI is on-site	Contact OI.
No OI on-site, but IRS-CI is on-site	Contact IRS-CI for immediate response, then follow-up contact with OI.
Neither OI or IRS-CI are on-site	Contact the local police department or FPS, as appropriate, for immediate response, then follow-up contact with OI.

Any victim, witness, or manager involved in a physical assault in the workplace should be advised of the following:

- Contact the most readily available law enforcement authority as directed above to ensure no further violence occurs;
- Ensure the assaulted employee receives immediate medical attention; and
- Notify OI of the incident.

260.16.2 Employee Right to File Complaint. Employees have the right to file a complaint with local police if they are threatened or assaulted in the workplace. Before filing, they may wish to discuss this option with their manager and/or OI.

Note: Formal referrals of TIGTA investigative products to State/local authorities or prosecutors should be made in accordance with the TIGTA Counsel guidelines in Section 70.5.2.

260.16.3 Response to Other Situations. IRS management is responsible for conducting any necessary inquiries and determining the appropriate action in the following situations:

- A verbal statement or gesture that does not include specific threats of harm or serious bodily injury is made to an employee;
- Inappropriate, but not threatening, statements and behavior are exhibited in the workplace; or
- Reports of harassment or intimidation by a fellow employee that does not involve sexual harassment allegations of quid pro quo or unwanted physical contact of a sexual nature.

Treasury Equal Employment Opportunity officials and IRS managers are required to report sexual harassment allegations to TIGTA. See Section 280.12.

IRS management is encouraged to contact OI for an assessment of the matter. After consultation, OI may take any of the following actions:

- Initiate an employee investigation;
- Refer the incident to local law enforcement authorities; or
- Refer the allegation back to IRS management for administrative action.

260.17 Employee Suicide Threats.
Suicide threats by employees could present a potential workplace violence situation. If OI receives a report of an employee suicide threat in the workplace, the following should be evaluated for safety considerations pertaining to the subject employee and other employees in the work area.

- Consider whether the employee has the means available to immediately cause harm (*e.g.,* weapons or items that could be used as weapons);
- Ascertain whether medical attention is needed;
- When possible, attempt to interview the employee pertaining to his/her intention to cause harm to him/herself and/or others;
- When possible, attempt to interview witnesses regarding the suicide threat;
- Consider contacting the local police department for transportation to a medical facility if the subject is combative/poses a danger to self or others;
- Consider use of on-site resources where available (*e.g.,* Health Unit, Employee Assistance Program).

The ASAC will evaluate the statements/actions of the employee and other pertinent circumstances and initiate an employee investigation when warranted. If an investigation is not warranted, the complaint should be referred to the IRS's Employee Conduct and Compliance Office for action.

Employee suicide threats should be documented in the CRIMES intake screen using violation code 161-Workplace Violence (IRS Employee Subject).

260.18 Employee Terminations or Other Adverse Actions.
Management may request OI's presence during employee terminations or other adverse actions.

Management should submit a request, via e-mail or telephone, to the responsible ASAC. Advise management of OI's role to ensure the safety of the manager and employee. OI may seek assistance from IRS-CI, on-site security, or other law enforcement personnel if additional support is needed. If a volatile contact has already commenced, or a delay in the termination may affect operations or safety, the SA receiving the request may provide immediate assistance but should notify the ASAC forthwith following the event.

TIGTA Form OI 7504 is **not** required.

DATE: April 1, 2021

CHAPTER 400 – INVESTIGATIONS

(400)-270 Bribery Investigations

270.1 Overview.
This section includes the following information related to bribery (and gratuity) investigations by the Office of Investigations (OI):

- Authority
- Initiating Bribery Cases
- Initial Actions
- Actions Prior to Bribery Meeting
- Bribery Meeting
- Arrest Procedures
- Post Bribery Meeting
- Referral Procedures
- Bribery Statutes
- Reporting Procedures

270.1.1 Acronyms Table.

270.2 Authority.
The Treasury Inspector General for Tax Administration (TIGTA) has specific jurisdiction to investigate bribery allegations involving employees of the Internal Revenue Service (IRS), IRS Chief Counsel, and the IRS Oversight Board. The authority of TIGTA is derived from the IRS Restructuring and Reform Act of 1998 and the Inspector General Act, as amended. The Plain Talk About Ethics and Conduct (IRS Document 12011) and Treasury Order 115-01 direct IRS employees to report bribery attempts directly to TIGTA.

Bribery, as defined in 18 U.S.C. § 201(b), is the giving or accepting of anything of value to or by a public official, if the thing is given "with intent to influence" an official act, or if it is received by the official "in return for being influenced." The giving or receiving of what are commonly known as gratuities is prohibited by 18 U.S.C. § 201(c). This subsection prohibits that same public official from accepting the same thing of value, if he does so "for or because of" any official act, and prohibits anyone from giving any such thing to him for such a reason.

When a bribe offer to an IRS employee occurs during a search or arrest by IRS Criminal Investigation (CI), IRS-CI will take appropriate action and notify TIGTA of the event as soon as possible. TIGTA will conduct the investigation in coordination with IRS-CI. See the Memorandum of Understanding between IRS-Criminal Investigation (CI) and TIGTA for investigative responsibilities regarding bribery.

270.3 Initiating Bribery Cases.
When an employee reports a bribe overture to TIGTA, initiate a Non-Employee Investigation in the Criminal Results Management System (CRIMES) using the appropriate violation code.

If a bribe is solicited by an employee, investigate the allegation as an Employee Investigation. The investigation must be initiated in CRIMES using the appropriate violation code.

270.4 Initial Actions.
Promptly interview the employee who reports the bribe offer or overture and obtain the following information from the employee:

- Information concerning the subject(s) offering the bribe;
- Brief general statement concerning the case or matter;
- Specific details of the bribe offer or bribe overture;
- Statements made by the employee; and
- Other pertinent information.

Note: Special agents (SA) should consider obtaining an affidavit from the employee; however, some Assistant U.S. Attorneys (AUSA) do not advocate obtaining an affidavit from an employee reporting a bribe overture. Determine the preference of the AUSA in your area. If the decision is made to obtain an affidavit, SAs will use the procedures outlined in Section 210.10.

Establish an investigative work plan based on all initial information provided and reviews of all available records.

In order to corroborate the employee's information and to preclude an entrapment issue, re-establish monitored contact with the subject as soon as practicable.

Obtain permission needed for electronic equipment using the procedures outlined in Section 170. Arrange for the use of technical equipment and necessary support personnel to operate the equipment.

270.4.1 Contacts with Cooperating Employee. A bribery investigation can be a stressful experience for a cooperating employee. SAs must provide support and attempt to alleviate fears or apprehension that an employee may have concerning the investigation. Empathize with the employee's work responsibilities and personal needs. These principles also apply to cooperating taxpayers, in circumstances where an employee is the subject of the investigation.

Encourage employee cooperation, as the investigation's success is dependent upon their participation; however, their participation is not required. Be aware of and discuss

with the cooperating employee factors that may affect him/her during the course of the investigation. SAs should be prepared to address any concerns that an employee may raise, *e.g.*, that in some cases participation in the investigation may cause the employee to:

- Interrupt assigned work, causing lowered productivity;
- Temporarily withhold information concerning the bribery investigation from supervisors;
- Cope with peer pressure and rumors;
- Discuss safety procedures;
- Have concern for personal and family safety; or
- Have concerns about doing something that may jeopardize the investigation.

Advise the employee that he/she may be asked to:

- Assume a role acting as a corrupt employee
- Make consensually monitored telephone calls
- Wear electronic equipment while conducting meetings with subject(s)
- Work unusual duty hours
- Testify for the Government in criminal proceedings

Stay in contact with employee throughout the process. Most employees are unaware and do not understand the process. Keep the employee advised of planned investigative and prosecutorial steps, and explain his/her role in these steps.

As appropriate, coordinate with the cooperating employee's management to ensure cooperation and assistance with administrative matters necessitated by the employee's participation in the investigation, *e.g.*, overtime, adjusted workdays, reduced caseload.

Provide emergency telephone numbers to the employee so he/she may contact the SA outside normal duty hours.

270.4.2 Entrapment Precautions. Entrapment is a complete defense to a criminal charge, on the theory that "Government agents may not originate a criminal design, implant in an innocent person's mind the disposition to commit a criminal act, and then induce commission of the crime so that the Government may prosecute."

The subject must have the opportunity as well as the intent to commit a crime.

If the LEO...	And...	Then...
Implants original intent in mind of subject		Entrapment
Gives subject opportunity to commit crime	The subject already intended to commit crime	No entrapment

Provide the cooperating employee examples of statements that do and do not constitute entrapment. Rehearse hypothetical situations the employee may encounter in meeting with the subject to help protect against entrapment and prepare for situations that may occur.

270.4.3 Coordinating with Other Internal Revenue Service Components. As necessary, the Special Agent in Charge will notify IRS functions of any bribe offer that may directly affect their function's responsibilities.

270.5 Actions Prior to Bribery Meeting.
Complete a briefing of the cooperating employee. The briefing process ideally begins 24 or 48 hours immediately preceding the bribery meeting. The case SA provides initial instructions and may complete role-playing exercises to familiarize the cooperating employee with situations likely to occur during the bribery meeting, as appropriate. Using specific "what if" situations alleviates the cooperating employee's apprehension and builds confidence. If possible, these role-playing exercises should be conducted more than once.

Coordinate checks of all technical investigative equipment with the Technical Support Officer (TSO) and Divisional Technical Agent (DTA). If feasible, the case SA should schedule a meeting between the TSO/DTA and cooperating employee to discuss proper attire and explain the equipment. Allow the cooperating employee to wear and test the equipment during the briefing process.

Provide adequate personnel resources to ensure the **safety** of all employees.

Prepare a written plan for the bribery meeting and ensure that each participant is aware of the plan. An approved TIGTA Form OI 7504, *Operational Plan*, is required.

Inventory the cooperating employee's personal belongings, including any money in his/her possession. If the cooperating employee uses a vehicle to travel to the bribery meeting, search the vehicle for any valuables and inventory them. Keep the cooperating employee and the vehicle under constant observation until the bribery meeting is concluded. Document the inventories in the TIGTA Form OI 6501,

Chronological Case Worksheet (CCW). Both pre and post inventories must be documented.

270.6 Bribery Meeting.
Conduct the bribery meeting outlining the **safety** of the cooperating employee and SAs as the first priority.

270.7 Arrest Procedures.
Arrests will be handled as outlined in Section 140.4.

270.8 Post Bribery Meeting.
After a bribery meeting:

- Keep the employee under continuous observation;
- Inventory the cooperating employee's personal belongings and vehicle used (if applicable), and document all inventories on the CCW;
- Recover and record the serial numbers of the bribe money;
- Secure bribe money using evidence procedures outlined in Section 190.3 of this Chapter; and
- Dispose of bribe moneys as outlined in Chapter 600, Mission Support, Section 50.11.5 of the TIGTA Operations Manual.

De-brief the cooperating employee.

Each contact with the employee (or cooperating taxpayer) is critical to the success of a bribery investigation. Refer to training materials and obtain advice based on the successful experience of other SAs and your management prior to conducting any briefing or de-briefing of a cooperating employee.

270.9 Referral Procedures.
Contact an AUSA early in the investigation and advise him/her of the investigative work plan.

The case SA should discuss with the AUSA the use of consensual electronic monitoring (audio or video) as an investigative technique. In situations, which the AUSA determines that TIGTA's use of consensual monitoring is legal and appropriate, the SA should prepare TIGTA Form OI 5177, *Request for Authorization to Use Electronic Equipment and Consensual Monitoring*. See Section 170.7.

Refer criminal violations to an AUSA as described in Section 250.14. If the bribe is of an IRS employee, SAs may consider referring bribery cases to the U.S. Department of Justice's Public Integrity Section, as appropriate.

270.10 Bribery Statutes.
Refer a bribe involving a thing of significant value under 18 U.S.C. § 201(b), which is a felony punishable by a fine or not more than three times the monetary equivalent of the thing of value, whichever is greater, or imprisonment for not more than 15 years, or both.

Refer a gratuity involving a thing of value under 18 U.S.C. § 201(c)(1)(A). This section carries only a fine or imprisonment for not more than two years, or both, and is a lesser included offense within bribery.

Other statutes which may be applicable are 18 U.S.C. § 371 and 18 U.S.C. § 203.

270.11 Reporting Procedures.
Prepare Reports of Investigation in accordance with Section 250.

DATE: October 1, 2017

CHAPTER 400 – INVESTIGATIONS

(400)-280 IRS Employee Investigations

280.1 Overview.
The Office of Investigations (OI) investigates complaints and allegations against Internal Revenue Service (IRS) employees. The results of investigations are submitted to IRS management without recommendation as to any action to be taken. Investigations of TIGTA employees are addressed separately in Section 330.

This section includes the following information related to employee investigations:

- Investigative Jurisdiction
- Complaint Procedures
- Initiating Employee Investigations
- Post-Appointment Arrest Investigations
- Allegations Requiring Internal Affairs Division (IAD) Coordination
- Investigative Procedures
- Reports of Investigations
- Conflict of Interest Referrals
- Recovering Unjust Enrichments
- Required Notifications Under 26 U.S.C. § 7431
- Sexual Harassment Allegations
- Tax and Financial Crime-Related Employee Misconduct

280.1.1 Acronyms Table.

280.2 Investigative Jurisdiction.
OI is responsible for detecting and investigating violations involving IRS employees and former employees. The employment status of the subject at the time the investigation is initiated is not relevant, only what his/her status was at any time during the time the violation was alleged to have been committed. An allegation must be related to the administration of the programs and operations of the IRS to be considered for investigation. See Section 10.3 for OI divisional responsibilities and duties.

280.2.1 IRS Employees Under TIGTA's Jurisdiction. OI is responsible for conducting investigations of alleged misconduct (as defined in Section 280.4) by all IRS employees, including, but not limited to:

- GM/GS employees;
- IR-1 employees;
- Office of Chief Counsel employees;
- IRS Oversight Board; and

- International employees.

See Section 210.5.1 of this chapter for a more detailed discussion of covered IRS employees. Also, please note that investigations of some of these IRS employees must be referred to OI's IAD). See Section 280.6.

280.3 Complaint Procedures.
Complaints should be entered into the Criminal Results Management System (CRIMES) within 15 days of receipt. The appropriate OI division will interview the complainant, evaluate all the information, and decide whether to initiate an investigation. See Section 240 for further information.

280.4 Initiating Employee Investigations.
OI will initiate an employee investigation if the allegation meets all of the following four elements:

- The complaint is against an identified IRS employee, or if the identity is unknown, against a person believed to be an IRS employee;
- The alleged violation occurred when the subject was employed by the IRS, regardless of the subject's employment status at the time the case is initiated;
- The allegation involves criminal or serious administrative misconduct; and
- There is a nexus between the alleged violation and the administration of the programs and operations of the IRS.

280.5 Post-Appointment Arrest Investigations.
Upon receipt of information concerning a post-appointment arrest of an identified employee, contractor, or someone believed to be an IRS employee or contractor, enter the initial intake in CRIMES and then verify the arrest.

280.5.1 Initiating a Post-Appointment Arrest Investigation. After verifying the arrest, the special agent (SA) will evaluate the complaint and initiate an investigation, when warranted. All post-appointment arrests concerning matters within TIGTA's jurisdiction will be considered for investigation, including arrests involving financial crimes, theft, or controlled substances. Arrests involving domestic violence are investigated when the subject is an IRS Criminal Investigation (IRS-CI) SA.

280.5.2 Notifying IRS of Post-Appointment Arrests. In all post-appointment arrests, the Special Agent in Charge (SAC) will notify the IRS as follows:

- If the post-appointment arrest information was received from the IRS's Employee Conduct and Compliance Office (ECCO), the SAC or the Assistant Special Agent in Charge (ASAC) will notify the IRS, via the two-way memorandum, whether OI will investigate the arrest. If no investigation is initiated by OI, the SAC will return the post-appointment arrest documents with the two-way memorandum.

- If the post-appointment arrest information was received from a source other than ECCO, and no investigation is initiated, the SAC will notify the IRS via Form OI 2070, Complaint Referral Memorandum.

280.6 Allegations Requiring Internal Affairs Division Coordination. Allegations made against IRS-CI employees, employees of the IRS Office of Chief Counsel, TIGTA employees, international IRS employees as defined in Section 340.2.2, or senior IRS officials as defined in Section 340.2.1 should be referred to the SAC-IAD for investigative consideration and coordination.

280.7 Investigative Procedures.
SAs will conduct a thorough analysis of the complaint or allegation and prepare an investigative work plan outlining all evident steps. SAs will place this information on the approved Form OI 6501, Chronological Case Worksheet. SAs will conduct all leads to prove or disprove the elements of the violation, or to show that the issue cannot be resolved. Refer to Section 250.4 for further instructions on investigative work plans.

280.7.1 Initial Interviews. Interview the complainant within 15 days. If extenuating circumstances prevent this, the SA should contact the complainant by telephone to arrange for a mutually convenient interview time.

The decision to interview or not interview an IRS employee who is the subject of an employee investigation should be made on a case-by-case basis. See Section 210.5 for a list of general guidelines. Where there is no reasonable indication that a criminal statute has been violated, the SA must consider interviewing the subject at the outset of the investigation.

280.7.2 Pledges of Confidentiality. Generally, OI does not extend an assurance of confidentially to any individual who may be involved in the violation being investigated. See Section 210.2.5 concerning pledges of confidentiality for witnesses and requirements for reporting such matters on a Form OI 2028-M, Memorandum of Interview or Activity. See also Section 150 for guidelines on the use of confidential sources (CS).

280.7.3 Granting Confidentiality. Pursuant to Section 210.4, all Department of the Treasury employees who are complainants or who have provided information concerning violations of law, rules, regulations and/or fraud, waste, and abuse, are presumed to have confidentiality under § 7(b) of the Inspector General (IG) Act, unless they specifically consent to allow TIGTA to disclose their identities. As a result, Treasury employees who furnish information to TIGTA and request confidentiality pursuant to the IG Act are processed as follows:

- Fully document the identity of the Treasury employee in CRIMES;

- Identify the employee in the Report of Investigation (ROI) by the temporary identifier T-1, T-2, etc., as the employee's identity should not be made known outside of TIGTA; and
- Check "No" to the "Confidentiality Waived" question in CRIMES.

280.8 Reports of Investigation.
SAs will close employee investigations and refer the ROIs for criminal prosecution or administrative adjudication promptly.

SAs will prepare ROIs as outlined in Section 250.7.

280.9 Conflict of Interest Referrals.
Pursuant to 5 U.S.C. app. 4 § 402(e)(2) and 5 CFR § 2638.603, TIGTA is required to report to the Director, Office of Government Ethics (OGE), possible violations of Federal conflict of interest statutes, 18 U.S.C. §§ 203, 205, 207, 208, and 209;a civil or criminal matter related to the filing or non-filing of a financial disclosure report under applicable legal authorities; or a civil matter involving outside earned income under 5 U.S.C app. 501 or outside activities under 5 U.S.C. app. 502. OGE requires a report whenever a potential violation of any of the above statutes is referred to the Department of Justice (DOJ) for criminal prosecution or civil enforcement. OI utilizes OGE Form 202, Notice of Conflict of Interest Referral, Part 1, Part 2 and Part 3 to fulfill this reporting requirement.

If the investigation was not referred for a violation of one of these statutes, do not submit an OGE Form 202.

280.9.1 OGE Form 202, Part 1. The OGE Form 202, Part 1 must be submitted after the initial referral, whether oral or written, to the U.S. Attorney's Office (USAO) or DOJ. Part 1 is intended to collect only basic information related to the open investigation to include:

- The name of the referring agency (TIGTA);
- The agency point of contact (Special Agent making referral);
- The identity of the DOJ component to which the referral was made (*i.e.,* the Public Integrity Section, the U.S. Attorney's office for a particular district, or another DOJ component);
- The date of the referral; and
- The TIGTA investigation number.

Upon receipt of OGE Form 202, Part 1, OGE will assign a tracking number and then confirm receipt of the referral and inform TIGTA of the assigned OGE tracking number. If the case agent, as the agency point of contact, receives notification of the assigned OGE tracking number, the SA should forward the OGE tracking number to Operation's

Inbox ***TIGTA Inv Operations**, within three days of receipt along with the TIGTA investigation Number.

280.9.2 OGE Form 202, Part 2. OGE Form 202, Part 2 must be submitted by the assigned SA after **both** of the following events have occurred:

- DOJ has a) declined prosecution; b) initiated prosecution or taken other legal action that is a matter of public record; or c) settled the matter through formal agreement; and
- Investigation of the matter has concluded.

OGE Form 202, Part 2 is intended to collect the following information:

- The identity of the subject employee;
- The name of the employing agency and component;
- The relevant legal authorities implicated by the alleged conduct;
- Actions taken, or determinations made, by DOJ; and
- Other information deemed pertinent by the referring office.

280.9.3 OGE Form 202, Part 3. OGE Form 202, Part 3 is intended to report, when applicable, the employing agency's administrative resolution to any related Ethics or Code of Conduct violations. Part 3 of Form 202, will be submitted by the Designated Agency Ethics Official (DAEO) of the employing agency. In most TIGTA investigations, the employing agency will be the IRS; therefore, the individual responsible for completing and submitting Part 3 of Form 202 will be the IRS' DAEO, or designated representative. If Part 3 of Form 202 becomes applicable, OGE will contact the employing agency's DAEO for submission of the form. **The assigned SA is not responsible for the completion or submission of Part 3 to OGE**.

Note: For TIGTA employee investigations, TIGTA's Office of Chief Counsel serves as the DAEO.

280.9.4 Reporting Procedures. Following all actions that require reporting, divisions must forward completed OGE Forms 202, Part 1 and Part 2 through the ASAC and SAC to the ***TIGTA Inv Operations** e-mail box by the 10th of each month. If the division has no conflict of interest referrals or subsequent actions to report for the month, a negative report is required and must also be sent to the ***TIGTA Inv Operations** e-mail box by the 10th of each month.

Note: Based on the particular facts of each case, it is possible the submission of OGE Form Part 1 and Part 2 will be submitted simultaneously. For example, if an investigation is referred orally to DOJ and declined; resulting in the investigation being immediately referred to the IRS for administrative action, then Part 1 and Part 2 will be submitted simultaneously.

OGE will contact TIGTA on a quarterly basis requesting status updates until OGE Form 202, Part 2 is received. The SAC is responsible for reporting a DOJ referral update, by the 10th of each month, for each pending investigation, when an OGE Form 202, Part 2 has not yet been submitted, describing the current status of the investigation, such as:

- Awaiting response from DOJ;
- DOJ declined prosecution, investigation pending;
- DOJ declined prosecution, investigation concluded (adverse ethics-related findings against the subject);
- DOJ declined prosecution, investigation concluded (no adverse ethics-related findings against the subject);
- DOJ initiated a criminal prosecution;
- DOJ initiated an action for civil penalties; or
- DOJ resolved the matter by agreement with the subject.

The SAC will provide one of the above status updates for each previously referred investigation as part of their normal monthly OGE reporting requirements.

Once OGE Form 202, Part 2 has been submitted, no further monthly monitoring or reporting is required.

Note: Before reporting cases involving undercover (UC) operations, electronic equipment usage and/or confidential grand jury information, coordinate with the Operations Division for guidance on reporting requirements.

The SAC-Operations will prepare a monthly memorandum to the Director, OGE, advising of any referrals and subsequent DOJ actions.

280.10 Recovering Unjust Enrichments.
As an alternative to, or in addition to, criminal prosecutions, civil sanctions should be pursued in any case involving employees or non-employees who were unjustly enriched. SAs should discuss civil and criminal aspects of their investigations with an Assistant United States Attorney (AUSA) to ensure that all possible sanctions available to the Government are pursued.

SAs should discuss debt collection activity with IRS officials following an employee's arrest, suspension, or removal when the employee may be indebted to the Government due to unjust enrichments. Coordinate with the AUSA in prosecution cases. See 26 U.S.C. § 7804 for additional information.

280.10.1 Notification in Theft and Embezzlement Cases.
In all investigations, including lockbox investigations, where TIGTA receives information that a theft or embezzlement of funds deposited with the IRS has occurred, notify the

IRS by memorandum from the SAC within 10 days of interviewing the complainant and making a determination that there is a reasonable basis to conclude a theft or embezzlement has occurred.

280.10.2 Notification When Financial Harm Has Occurred. Generally, if financial harm to a taxpayer has occurred, notify the IRS immediately so that appropriate action can be taken to make the taxpayer whole. In cases where the affected taxpayers have been identified, the SAC will provide the IRS with a list of the taxpayers so that the IRS can protect the taxpayers from any undue collection activity. The SAC will send the memorandum to the Field Director of the Submission Processing Center that services each taxpayer's account. The memorandum must contain the following available information:

- Assigned case number;
- Taxpayer's name, identification number, type of tax, tax period, and amount and date of payment;
- Request that the taxpayer's account be credited;
- Where the theft/loss occurred;
- Status of the remittance; and
- The name and telephone number of the SA.

If, during the investigation, the IRS needs information that was not available when the initial notification was given, direct the IRS to contact the SA identified in the initial memorandum. If the information is provided verbally by the SA, the IRS may request that the verbal information be confirmed in writing by a memorandum. When verbal information is requested in writing, the SAC will provide the Field Director of the respective Submission Processing Center with a memorandum detailing the updated information.

See Exhibit(400)-280.1 for sample format of memorandum to a Field Director, Submission Processing Center.

See Exhibit(400)-280.5 for Submission Processing Center addresses.

280.10.3 Final Notifications in Theft and Embezzlement Cases. At the completion of an investigation involving a theft or embezzlement, notify the IRS of the final results of the investigation, including the results of any prosecution and sentencing so that the IRS can determine when to initiate collection action and the amount to be assessed.

The SAC will send a memorandum of the results of prosecution and sentencing to the Field Director of the Submission Processing Center that services each taxpayer's account. The memorandum will contain the following:

- Subject's name;

- Disposition of the case (*e.g.*, guilty, not guilty, pretrial diversion);
- Sentence (*e.g.*, length of incarceration or probation, or amount of court-ordered restitution, fines, and court costs); and
- If applicable, notification that TIGTA is transferring tax remittance money to the IRS that was seized during the investigation and forfeited by the court to TIGTA.

When tax remittance money is seized during a theft or embezzlement investigation, the case SA should request the court to order that the money be forfeited to TIGTA so TIGTA can transfer it to the IRS for deposit into the Treasury General Fund to be credited to the affected taxpayers' tax accounts. If the court orders the forfeiture of the seized tax remittance money to TIGTA, the SA must convert the cash money to a cashier's check or money order made payable to the U.S. Department of the Treasury. The SAC will forward the check or money order with the results memorandum and attach an IRS Form 3210, Document Transmittal that contains the following information:

- **To Block:** IRS Submission Processing Center Address where the results memorandum is being sent.
- **Document Identification Block:** Seized tax remittance money, case number, cashier's check or money order number, made payable to the U.S. Department of the Treasury, and the amount.
- **Remarks Block:** Overnight tracking number.
- **From Block:** Case SA's mailing address.
- **Releasing Official Block:** SAC signs.

The Form 3210, results memorandum, and check or money order must be sealed in an inner "Confidential" envelope and mailed to the IRS using traceable overnight mail.

Once the signed Form 3210 is received from the IRS, the SA must attach the signed Form 3210 to a Statement of Special Moneys and Property Transaction (Form OI 141), as supporting documentation for disposal of the money. See Form OI 141 instructions for preparation and disposition of the form, and Chapter 600, Section 50.11.4 and for receipt and disposal of special moneys.

See Exhibit(400)-280.4 for the format of the memorandum of prosecution and sentencing to a Field Director, Submission Processing Center.

See Exhibit(400)-280.5 for Submission Processing Center addresses.

The SAC will prepare a memorandum transmitting the final ROI to the Field Director of the Submission Processing Center that services each taxpayer's account and attach to it a copy of the ROI. The transmittal memorandum, ROI, and Form OI 2076, Referral Memorandum is then sent to IRS Employee Conduct and Compliance Office (ECCO) as instructed in Section 250.12.1. If the IRS Remittance Security Coordinator or the Field

Director, Submission Processing Center requests more information, direct them to contact the originating SAC directly.

See Exhibit(400)-280.3 for the format of the memorandum transmitting the final ROI to a Field Director, Submission Processing Center.

280.10.4 Court Ordered Restitution. The IRS has designated a centralized office to collect and process all criminal restitution payments in which the IRS is a victim of crime, and has coordinated this procedure with the U.S. Courts, the U.S. Probation offices, and the U.S. Attorney's offices. In cases where the court orders restitution as a part of sentencing, advise the AUSA's office and the U.S. Probation office that restitution payments should include the affected taxpayer's full name and the court docket number, and should be sent to the following address:

Internal Revenue Service
Attn: MS 6261 Restitution
333 W. Pershing Rd.
Kansas City, MO 64108

280.10.5 Stopping Payment of Money Due an Employee. The IRS has authority to withhold payments of salary and benefits of an employee, including the final salary payment of a separating employee who has been found to have embezzled or stolen Government funds. The requests are processed by the National Finance Center (NFC) through the IRS's Austin Payroll Center. NFC establishes a debt related to the embezzled or stolen funds and sends a notification to the employee. If the employee subsequently separates, their final paycheck or lump sum payout is offset and applied to the debt. To request the IRS consider such an offset of funds, the SA should:

- Obtain concurrence from the AUSA prosecuting the case;
- Keep the AUSA apprised of the status of the employee to ensure that criminal prosecution is not influenced by any administrative action; and

Mail a formal request memorandum from the SAC to:

Chief of the Austin Payroll Center
3651 S. IH 35, Stop 1557 AUSC
Austin, TX 78741

The subject line should read, Request to establish a debt as a result of a TIGTA investigation.

The memorandum must include the following information:

- Agency;
- Name of debtor (employee);

- Payroll Office Identifier (POI)/employee organization code;
- Social Security Number of debtor;
- Date of Birth;
- Address of debtor;
- Current employment status;
- Amount of debt;
- Fiscal year of the debt; and
- Reason for the debt.

See Exhibit(400)-280.2 for a sample format of the memorandum to the Chief, Austin Payroll Processing Center.

In cases where TIGTA funds are embezzled or stolen during a remittance test, the above procedures of stopping payment also apply. For further information on remittance tests see Section 390.

280.11 Required Notifications Under 26 U.S.C. § 7431.
Upon the filing of a criminal information or indictment for unauthorized access or disclosure under 26 U.S.C. § 7213, 26 U.S.C. § 7213A, or 18 U.S.C. § 1030(a)(2)(B), the SAC-Operations, upon notification from the field, will provide the information to the IRS Privacy, Governmental Liaison and Disclosure, which will notify the affected taxpayer(s) pursuant to the notification provision of 26 U.S.C. § 7431(e). For further information on 26 U.S.C. § 7431 notifications to the IRS, see Section 290.9.

280.12 Sexual Harassment Allegations.
TIGTA is responsible for investigating the following types of sexual harassment allegations at the IRS:

- Quid pro quo situations, in which submission to or rejection of sexually harassing behavior is used as a basis for employment decisions affecting the employee. Examples of quid pro quo behavior include promises of a promotion for engaging in sexual activity, negative appraisals for refusing to engage in sexual activities, or employment action taken against an employee for refusing to engage in sexual activities;
- Unwanted physical contact of a sexual nature; and
- Conduct of a sexual nature for the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.

280.12.1 IRS Policy and Authority. IRS policy is to provide a work environment free from sexual harassment. Sexual harassment will not be tolerated, whether committed by executives, supervisors, employees, or non-employees such as contractors, taxpayers, or visitors.

Sexual harassment is:

- Illegal under Title VII of the Civil Rights Act of 1964, as amended;
- Defined in Equal Employment Opportunity Commission (EEOC) regulations, 29 C.F.R. § 1604.11; and
- Specifically prohibited by Treasury Employee Rules of Conduct, 31 C.F.R. § 0.214.

280.12.2 Reporting Sexual Harassment Allegations. An IRS employee can report sexual harassment through any of the following methods:

- The statutory EEO complaint process, which includes EEO counseling and the option of simultaneously bringing the allegation to the attention of the Commissioner and TIGTA;
- The Treasury Hotline 800-359-3898;
- Contact with IRS management such as a supervisor or head of office;
- The negotiated grievance process for bargaining unit employees; or
- The toll-free TIGTA Hotline 800-366-4484 or direct contact with TIGTA if the sexual harassment involves quid pro quo circumstances or unwanted physical contact of a sexual nature.

A victim is not required to report sexual harassment allegations to TIGTA. However, EEO officials and IRS managers to whom allegations are reported are required to refer to TIGTA those allegations meeting the criteria set forth in Section 280.12.

280.12.3 Relationship Between EEO and TIGTA Investigations. A victim may report an allegation of sexual harassment to both TIGTA and EEO. Employees may continue to seek a remedy under the statutory EEO complaint process even if a TIGTA investigation is initiated.

Separate TIGTA and EEO investigations may be conducted simultaneously regarding the same incident. The referral to TIGTA does not suspend the EEO process and an EEO investigation does not suspend the TIGTA investigation.

SAs will explain to complainants that a TIGTA investigation is not the same as an EEO investigation and that:

- Victims are not required to report the allegation to EEO;
- If EEO remedies are desired, victims making a sexual harassment complaint to TIGTA must contact an EEO counselor within 45 days of the alleged harassment to preserve their EEO rights; and
- TIGTA investigations concentrate on the issue of employee misconduct, while EEO investigations concentrate on resolving the alleged workplace discrimination.

When a victim initially reports an allegation to EEO that meets the criteria for referral to TIGTA, EEO informs the victim that:

- A referral to TIGTA will be made;
- His/her identity will not be revealed without his/her written authorization; and
- His/her request to be anonymous may limit IRS management's ability to conduct an inquiry or resolve the allegations.

If the victim does not consent to reveal his/her name, EEO refers the allegation to TIGTA, but maintains the anonymity of the victim.

Note: Once an employee files a formal complaint in the EEO process, he/she has no right to anonymity.

Do not provide EEO investigators with a copy of a TIGTA ROI, allow them to review the ROI, or disclose the existence of an investigation. Refer all EEO investigator requests for TIGTA documents to the TIGTA Disclosure Officer. See Chapter 700, Chief Counsel, Section 20.3 of the TIGTA Operations Manual for an overview of the responsibilities of the TIGTA Disclosure Branch.

280.12.4 Case Initiation Procedures. SAs will document the receipt of any complaints regarding sexual harassment, regardless of the source. Forward the allegation to the ASAC for evaluation. If communicated verbally, document the complaint in writing on Form OI 2028-M, Memorandum of Interview or Activity to the ASAC.

The ASAC evaluates allegations of sexual harassment to determine if the circumstances warrant a TIGTA investigation. While not every sexual harassment allegation warrants a TIGTA investigation, an investigative determination is made in every complaint meeting the criteria in Section 280.12. TIGTA officials may consult with EEO officials to determine whether the allegations meet either of the two criteria. After this threshold determination, the ASAC decides whether the allegation should be investigated by OI. The ASAC forwards the information to the SAC-Field Division or, in the case of a TIGTA employee, to the SAC-IAD, for concurrence prior to initiating an investigation.

Note: The SAC must concur before an investigation is initiated. The ASAC will document this concurrence and its date in the "Remarks" section in CRIMES.

Use Violation Code "590 – Sexual Harassment" in CRIMES to indicate quid pro quo or touching allegations.

Use Violation Code "952 – EEO Issue/Sexual Harassment" in CRIMES for sexual harassment allegations that may be administrative in nature (*e.g.*, verbal comments).

280.12.5 Notifying IRS Management. Prompt notification to IRS management allows for immediate and appropriate corrective action in cases of sexual harassment. Within five workdays of receiving the complaint, the SAC or his/her designee will notify IRS management concerning OI's decision to:

- Initiate an investigation to resolve the sexual harassment complaint; or
- Not investigate the sexual harassment complaint.

280.12.6 Sexual Harassment Allegations Requiring IAD Coordination. Allegations made against IRS-CI employees, employees of the IRS Office of Chief Counsel, TIGTA employees, international IRS employees as defined in Section 340.2.2, or senior IRS officials as defined in Section 340.2.1 must be referred to the SAC-IAD.

280.12.7 Investigations of Sexual Harassment. Absent unusual circumstances:

- SAs will complete sexual harassment investigations within 45 days after receipt of a complaint; and
- SAs will give sexual harassment investigations a high priority.

SAs must:

- Establish an investigative strategy upon receipt of the case; and
- Consider the benefit of having an SA of the opposite sex assist in conducting the investigation.

A victim is not required to provide testimony in instances where third parties have provided the sexual harassment complaint or allegation. A victim's right to confidentiality must be maintained at all stages of the investigative process and will only be disclosed on a "need to know" basis. While there are no Federal criminal statutes that directly address quid pro quo sexual harassment, consider the elements of the case and other Federal statutes that may fit the circumstances, such as blackmail, extortion, bribery or gratuities.

The following reference material may be helpful when investigating allegations of sexual harassment:

- IRS Document 12011, Plain Talk About Ethics and Conduct;
- The Equal Employment Opportunity Commission;
- U.S. EEOC Regulations, 29 C.F.R., Part 1614;
- U.S. EEOC Management Directive 110, Federal Sector Complaint Processing Manual; and
- 18 U.S.C. § 2241, 18 U.S.C § 2242 and 18 U.S.C. § 2245.

280.12.8 Referral for Administrative Adjudication. When referring a TIGTA ROI involving sexual harassment to IRS management, the SA will make the following annotation in the "Remarks" section of Form OI 2076: "**This Report of Investigation involves a matter in which there may be related EEO activity**."

280.13 Tax and Financial Crime-Related Employee Misconduct.
Allegations of misconduct by IRS or TIGTA employees, including tax and financial crimes involving employees, fall within the investigative responsibility of TIGTA. TIGTA investigations of employees for Title 26 **tax-related** violations require coordination with IRS-CI and the Department of Justice Tax Division (DOJ-Tax). Examples would include, but are not limited to, IRS employees involved in refund schemes, and IRS employees filing false tax returns. DOJ-Tax has authorized direct referral to the local U.S. Attorney's Office on a limited number of Title 26 violations, such as unauthorized access (UNAX) and unauthorized disclosure. See Section 350.3 for a list of direct referral violations.

280.13.1 Coordination with IRS-CI. TIGTA SAs should request assistance from IRS-CI for tax and financial crime-related employee misconduct. Although IRS-CI has been delegated responsibility for investigating substantive tax and related offenses, the overriding goal of the IRS to maintain the integrity of its workforce makes TIGTA involvement in these investigations necessary. Disputes involving joint investigations of IRS personnel ultimately will be resolved by TIGTA. Additional information on investigative responsibilities is outlined in the Memorandum of Understanding (MOU) between the IRS and TIGTA. See the DOJ-Tax Referral Matrix, Exhibit (400)-350.1, for situations requiring referral to DOJ-Tax.

The general filing of fraudulent tax returns using stolen identities is within the jurisdiction of IRS-CI. However, IRS employee involvement in an identity theft scheme - either through UNAX, disclosure, or as a participant in the criminal activity, falls within TIGTA's jurisdiction. Allegations of employee involvement in a stolen identity refund scheme should be coordinated with IRS-CI. DOJ-Tax Directive 144 has delegated certain authority regarding Stolen Identity Refund Fraud (SIRF) investigations directly to participating U.S. Attorney's Offices without prior approval by DOJ-Tax. The purpose of the delegation is to provide Federal law enforcement officials with the ability to timely address SIRF crimes. The directive allows for expedited local processes, (*e.g.*, empaneling a tax grand jury, arresting and Federally charging suspects by criminal complaint), but still requires some coordination with DOJ-Tax. See the directive for additional information and specific parameters of the delegation.

280.13.2 Substantive Tax or Financial Offenses. In cases where IRS or TIGTA employees are allegedly committing substantive tax or financial offenses, such as filing false returns or other tax-related documents, willfully failing to file returns or pay taxes, willfully attempting to evade the assessment or payment of taxes, filing false claims for

refunds – including identity theft schemes, conspiring to defraud the U.S., or to commit an offense against the U.S. ("Klein conspiracy"):

- TIGTA contacts IRS-CI to obtain assistance in investigating the substantive tax and financial aspects of the allegations. TIGTA's request for assistance in such investigations is normally made by the ASAC, with the concurrence of the SAC, to the appropriate IRS-CI management official;
- TIGTA requests an SA from IRS-CI be assigned to assist in evaluating and, if appropriate, conducting the investigation for substantive tax or financial offenses; and
- The assigned IRS-CI SA will investigate allegations pursuant to CI's delegated responsibilities to investigate substantive tax and related offenses.

If any substantive tax or financial crime investigation is independently initiated by IRS-CI and is found to involve an IRS/TIGTA employee:

- IRS-CI will immediately notify TIGTA of the allegations; and
- The TIGTA SA will prepare a Form OI 2028-M, which will be placed in the investigative file to document the notification.

If employee tax violations are alleged to have been committed by an IRS-CI employee:

- The information will be provided by the responsible TIGTA SAC to the responsible IRS-CI Director of Field Operations (DFO); and
- The DFO will ensure the IRS-CI SA assigned to work on the investigation is from a district other than the district in which the targeted IRS-CI employee is assigned.

If IRS-CI declines to participate in an investigation and TIGTA disagrees with CI's decision, the ASAC/SAC should elevate the issue to the appropriate DAIGI for further review and consideration. The last right of refusal is reserved for the Inspector General.

In a joint investigation with IRS-CI, the TIGTA investigative report may be submitted to DOJ-Tax as an inclusion to IRS-CI's report or separately, depending on the circumstances of the case. The appropriate DOJ-Tax Enforcement Division should be contacted for guidance. Separate referrals may be necessary due to the need for a timely submission or other case specific factors. If the case involves an IRS employee subject and TIGTA has primary jurisdiction, then TIGTA should submit a separate report or include the CI report as an inclusion to TIGTA's report. If TIGTA makes a separate referral to DOJ-Tax, ensure the referral states that IRS-CI will be referring its case at a later date. If IRS-CI has primary jurisdiction and the referral is made jointly, the responsible SAC will forward the TIGTA ROI to the local IRS-CI SAC for inclusion with IRS-CI's referral to DOJ-Tax.

If, after initial review of an employee tax allegation, the IRS-CI SA working with TIGTA believes that no criminal tax violation has occurred:

- The IRS-CI SA should consult with IRS-CI management for concurrence and advise TIGTA accordingly;
- If TIGTA concurs that no criminal tax violations have occurred, the IRS-CI SA will share his/her investigative findings with TIGTA and provide a report to TIGTA summarizing the tax issues and investigative activity to date;
- The IRS-CI SA will not include conclusions or recommendations in the report; and
- If approved by TIGTA management, the IRS-CI report will become an attachment to the TIGTA ROI.

This same process will be followed if IRS-CI conducts an investigation, but does not believe there is a reasonable probability of conviction on tax charges and chooses to discontinue its investigation.

280.13.3 Referrals to DOJ-Tax. When appropriate in the course of an investigation, TIGTA SAs will utilize Form OI 8107, Request for Grand Jury Investigation, to request authorization from DOJ-Tax to empanel a tax grand jury. Use of this request would be appropriate if TIGTA wants to issue grand jury subpoenas or wants to include another (non-IRS) agency in the investigation. Typically, if IRS-CI is joining the investigation, authorization of a tax grand jury is part of CI's normal protocol; however, TIGTA is not precluded from requesting the authorization and circumstances may deem it appropriate. Provide the information as requested in the form and instructions and mail the form to DOJ-Tax at the address indicated in Block 1 of the form.

Either a Form OI 8107 or a DOJ-Tax prosecution authorization (via a referral letter) is required prior to an SA making any specific and substantive tax disclosures directly to an AUSA. Examples of DOJ-Tax Grand Jury Requests and/or Referral Letters can be found in the DOJ Tax Library link on the OI webpage.

If CI declines to investigate an employee tax-related allegation, contact with DOJ-Tax by TIGTA is still necessary to obtain authorization for prosecution by the local U.S. Attorney's Office (Form 8108), or a declination (Form 8110). Additional information regarding the process and forms for DOJ-Tax referrals can be found in Section 350.7 and Exhibit (400)-350.3. See Example DOJ-Tax Referral Letter.

Since both administrative and criminal violations may be present on employee tax cases, *i.e.*, a violation of 26 U.S.C. § 7206 may also be a potential violation of RRA 98 § 1203(b)(9), any subject interview of an IRS or TIGTA employee regarding false statements on his/her tax return should be conducted using OI Form 5230, Advisement of Rights - Non-Custodial, **unless prosecution has been declined** by the appropriate DOJ-Tax authority. If applicable, obtain a prosecutive declination on employee cases

from DOJ-Tax by completing Form OI 8110, Referral for Prosecutive Declination and Kalkines Warning Authorization, and mail to the address indicated in Block 1 of the form. DOJ-Tax will return the form to the requesting office with a prosecutive decision. After DOJ-Tax has declined prosecution and authorized the use of the Kalkines Warning, interviews of the employee should be conducted using Form OI 8112, Statement of Rights and Obligations.

280.13.4 Requesting Employee Audits. When an investigation declined by IRS-CI and DOJ-Tax includes allegations that an IRS or TIGTA employee's own personal tax return may contain false statements and/or an understatement of tax liability, request an employee audit to determine if the employee has violated a rule of conduct, including a potential violation of § 1203(b)(9) of RRA 98. The SA will request a tax audit by following the procedures outlined in Section 250.23.

The employee audit generally will be requested after the case has been declined for prosecution, but the timing of the audit may depend on the specific circumstances of the investigation. Discuss the circumstances with the ASAC/SAC/IRS-CI to ensure a civil audit referral will not jeopardize the criminal case, when applicable. If declined for prosecution, refer for employee audit in order to facilitate an administrative adjudication. Investigations that have been declined can be reconsidered criminally if false information is supplied in the audit or if criminal activity continues.

IRS will provide the results of the employee audit to the TIGTA office or individual identified in the requesting memorandum. Upon receipt of the audit results for IRS employees, the SA will prepare a final ROI, including the results of the audit, and forward the ROI to IRS ECCO for adjudication as instructed in Section 250.12. Ensure the subject interview has addressed the willfulness of the employee's actions. If the initial subject interview was conducted prior to the audit, an additional interview may be necessary to address willfulness.

ROIs that allege violations of RRA § 1203 (b)(9) should not be forwarded to IRS ECCO without audit results. IRS is unable to adjudicate this type of allegation without the audit results.

DATE: January 1, 2020

CHAPTER 400 – INVESTIGATIONS

(400)-290 Unauthorized Disclosure/Inspection Investigations

290.1 Overview.
The Office of Investigations (OI) evaluates allegations to determine if unauthorized disclosure or inspection of tax returns or return information has occurred. This section addresses:

290.1.1 Acronyms Table.

290.1.2 Definitions. This section contains the following terms:

Unauthorized Disclosure. An unauthorized disclosure is a disclosure of return or return information that is not authorized by Title 26.

Unauthorized Access or Inspection (UNAX). A UNAX is an access or inspection of return or return information that is not authorized by Title 26.

Return. Return means “any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed.” See 26 U.S.C. § 6103(b)(1).

Return Information. The term “return information” means:

(A) A taxpayer's identity, the nature, source, or amount of income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the

determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense;

(B) Any part of any written determination or any background file document relating to such written determination as such terms are defined in 26 U.S.C. § 6110(b) which is not open to public inspection under 26 U.S.C. § 6110;

(C) Any advance pricing agreement entered into by a taxpayer and the Secretary and any background information related to such agreement or any application for an advance pricing agreement; and

(D) Any agreement under § 7121, and any similar agreement, and any background information related to such an agreement or request for such an agreement.

Such term does not include data in a form which cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer. Nothing in the preceding sentence, or in any other provision of law, shall be construed to require the disclosure of standards used or to be used for the selection of returns for examination, or data used or to be used for determining such standards, if the Secretary determines that such disclosure will seriously impair assessment, collection, or enforcement under the internal revenue laws." See 26 U.S.C. § 6103 (b)(2).

Note: The Supreme Court unanimously ruled in *Church of Scientology v. IRS* that information protected by 26 U.S.C. § 6103 retains its protected character even if direct and indirect identifiers are removed.

Taxpayer Identity. Taxpayer identity is defined as “the name of a person with respect to whom a return is filed, his mailing address, his taxpayer identifying number (as described in § 6109), or a combination thereof.” See 26 U.S.C. § 6103 (b)(6).

290.2 Authority.
Section 9(a) of the Inspector General (IG) Act of 1978, 5 U.S.C. Appendix 3, transfers the Office of Chief Inspector of the Internal Revenue Service (IRS) and its functions, powers, and duties to the Treasury Inspector General for Tax Administration (TIGTA). Section 9(b) transfers the authorizations of the Office of Chief Inspector of the IRS to TIGTA. Treasury Order 115-01 gives TIGTA the duty and responsibility to conduct investigations relating to the programs and operations of the IRS. Treasury Order 115-01 also gives TIGTA the authority to enforce criminal provisions of the internal revenue laws and other criminal provisions of law relating to internal revenue for the enforcement of which the Secretary is responsible, among others. See 26 U.S.C. § 7608(b).

Section 6-4.200 - Tax Division Jurisdiction and Procedures of the Justice Manual (JM) provides that, "The Assistant Attorney General, Tax Division, has responsibility for all criminal proceedings arising under the internal revenue laws, with the exception of proceedings that pertain to unauthorized disclosure of information (26 U.S.C. § 7213)." This language means that alleged violations of § 7213 shall be taken to the United States Attorney. According to the JM, Section 9-79.420 - Disclosure Violations—Tax Reform Act of 1976 (26 U.S.C. § 7213), "United States Attorneys are required to consult with the Public Integrity Section of the Criminal Division before instituting grand jury proceedings, filing an information, or seeking an indictment of disclosure violations under 26 U.S.C. § 7213."

290.3 Statutory Protections of Confidential Taxpayer Information.
Congress enacted 26 U.S.C. § 6103 to establish the confidentiality of tax returns and tax return information. Congress also passed laws establishing criminal penalties and creating civil causes of action for violations of § 6103 to be used to enforce the protections of § 6103. For example:

- 26 U.S.C. § 7213 makes it a felony for a current or former Federal, State, or other government employee, or a contractor providing tax administration services under § 6103(n), to willfully disclose tax returns or tax return information in a manner not authorized by Title 26.

- 26 U.S.C. § 7213A makes it a misdemeanor for current Federal, State, or other government employees, or a contractor providing services under 26 U.S.C. § 6103(n), to willfully inspect tax returns or tax return information except as authorized by Title 26.

- 26 U.S.C. § 7431(a)(1) permits a taxpayer to bring a civil action for damages against the United States if a Federal or other non-Federal employee knowingly, or by reason of negligence, inspects or discloses that taxpayer's return or return information in violation of 26 U.S.C. § 6103.

290.4 Criminal Disclosure and Inspection Statutes.
Criminal disclosure and inspection investigations are based on alleged violations of the following statutes:

- 26 U.S.C. § 7213 – *Unauthorized disclosure of information* (tax information);
- 26 U.S.C. § 7213A – *Unauthorized inspection of returns or return information*;
- 26 U.S.C. § 7216 – *Disclosure by a tax return preparer*;
- 18 U.S.C. § 1030(a)(2)(B) – *Fraud and related activity in connection with computers*. If the computer access is to tax return information, the initiating statute should be 26 § 7213 or § 7213A; and

- 18 U.S.C. § 1905 – *Disclosure of confidential information generally* (other than tax return information.

290.4.1 26 U.S.C. § 7213. The elements of an offense under 26 U.S.C. § 7213 *Unauthorized disclosure of information*, as applied to Federal, State, or other government employees, are:

- A current or former officer or employee of the United States, a State, or other government agency in possession of returns or return information from the IRS or contractor providing tax administration services under 26 U.S.C. § 6103(n);
- Who willfully discloses;
- Tax returns or return information; and
- In violation of Title 26.

290.4.1.1 Statute of Limitations. In general, the statute of limitations is three years from the date of the offense, as provided in 26 U.S.C. § 6531, unless the indictment is found or the information instituted within three years next after the commission of the offense.

290.4.1.2 Penalties. The penalties upon conviction under 26 U.S.C. § 7213 include imprisonment for not more than five years, a fine not to exceed $5,000, or both, and the costs of prosecution. Conviction results in dismissal from office or discharge from employment.

290.4.2 26 U.S.C. § 7213A. The elements of an offense under 26 U.S.C. § 7213A *Unauthorized inspection of returns or return information*, as applied to Federal, State, or other government employees are:

- An officer or employee of the United States, a State, or other government agency in possession of returns or return information from the IRS or contractor providing tax administration services under 26 U.S.C. § 6103(n);
- Who willfully inspects (see 26 U.S.C. § 6103(b)(7));
- Any return or return information (see 26 U.S.C. § 6103(b)(1) and (b)(2)); and
- In violation of Title 26.

290.4.2.1 Statute of Limitations. In general, the statute of limitations is three years from the date of the offense, as provided in 26 U.S.C. § 6531, unless the indictment is found or the information instituted within three years next after the commission of the offense.

290.4.2.2 Penalties. Penalties upon conviction include a fine not exceeding $1,000, imprisonment for not more than a year, or both.

290.4.3 26 U.S.C. § 7216. The elements of an offense under 26 U.S.C. § 7216, disclosure or use of information by preparers of returns, are:

- Any person in the business of preparing, or providing services in connection with the preparation of tax returns, or any person who for compensation prepares any such return for any other person;
- Who knowingly or recklessly discloses; and
- Any information furnished for, or in connection with, the preparation of a tax return; or uses the tax preparation information for any purpose other than to prepare or assist in preparing a return.

290.4.3.1 Statute of Limitations. In general, the statute of limitations is three years from the date of the offense, as provided in 26 U.S.C. § 6531, unless the indictment is found or the information instituted within three years next after the commission of the offense.

290.4.3.2 Penalties. A violation of this section is a misdemeanor punishable by imprisonment for not more than one year, a fine of not more than $1,000, or both; and the costs of prosecution.

290.4.4 18 U.S.C. § 1030(a)(2)(B). The elements of an offense under 18 U.S.C. § 1030(a)(2)(B), *Fraud and related activity in connection with computers*, are:

- Any individual – not necessarily an employee or agent of the United States;
- Who intentionally accesses a computer;
- Without authorization or exceeding authorization; and
- Obtains information from any department or agency of the United States.

290.4.4.1 Statute of Limitations. In general, the statute of limitations is five years after the date of the alleged offense, as provided in 18 U.S.C. § 3282.

290.4.4.2 Penalties. The penalties upon conviction may include imprisonment for up to 10 years, a fine, or both depending on the conviction history of the individual and certain factual characteristics of the offense. See 18 U.S.C. § 1030(c) and 18 U.S.C. § 3571.

290.4.5 18 U.S.C. § 1905. The elements of an offense under 18 U.S.C. § 1905 *Confidential information other than tax returns or return information*, are:

- Whoever, being an officer or employee of the United States or of any department or agency thereof;
- Publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law;

- Any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof;
- Which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or
- Permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law.

Anyone who violates this section shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.

290.5 Administrative Violations.
In addition to possible criminal violations, IRS employees' unauthorized disclosures of confidential taxpayer information are a violation of 31 C.F.R. Part 0, *Department of the Treasury Employee Rules of Conduct*, and IRS Document 12011, *Plain Talk About Ethics and Conduct.*

290.6 Reporting Unauthorized Disclosure/UNAX Violations.
UNAX allegations involving the following employees, regardless of their source must be reported as follows:

If...	Then...
A TIGTA employee,	Report the allegation directly to the Special Investigations Unit (SIU).
A GS-15 or higher IRS employee,	Report the allegation directly to SIU.
An IRS employee in the International (U.S. Competent Authority) function and is located in Washington, D.C. or U.S. embassies abroad,	Report the allegation directly to SIU. Agents should be aware of the exemption under 26 U.S.C. § 6103 to disclose return or return information to intelligence agencies.
An IRS employee in the International (U.S. Competent Authority) function and is located in Puerto Rico or the U.S. Virgin Islands,	Input the intake into the Criminal Results Management System (CRIMES) and transfer it to the SAC-Southern Field Division.

An IRS employee in the International (U.S. Competent Authority) function and is located in Guam or the American Samoa Islands,	Input the intake into CRIMES and transfer it to the SAC-Western Field Division.

Unauthorized disclosure or UNAX allegations involving all other IRS employees and non-employees will be entered into CRIMES and transferred to the SAC of the division responsible for the area in which the subject works or resides.

290.7 Initiation and Referral of Investigations.
The type of investigation initiated and the referral procedures are based on:

- The status of the subject at the time the alleged misconduct occurred; and
- The specific statutory violation.

All allegations relating to unauthorized disclosure and inspection violations should be documented in CRIMES using the appropriate UNAX/Disclosure violation profile and code. Contact the *TIGTA Inv Operations Inbox to resolve any questions regarding disclosure investigations.

290.7.1 IRS Employee. Follow the steps listed in the table below if the person alleged to have committed a disclosure or unauthorized access violation was an IRS employee at the time the unauthorized disclosure or inspection is alleged to have occurred:

If an IRS employee...	Then...
Violates 26 U.S.C. § 7213,	• Contact TIGTA Office of Chief Counsel (Counsel), if necessary; • Initiate and conduct an employee investigation; • Refer to the appropriate U.S. Attorney's Office (USAO); and • Refer to the IRS.
Violates 26 U.S.C. § 7213A,	• Submit a Request Assistance Form (RAF) via CRIMES to the Strategic Data Services Division (SDS) for UNAX analysis, as necessary; • Initiate and conduct an employee investigation, if warranted; • Refer to the appropriate USAO; and • Refer to the IRS.

Violates 26 U.S.C. § 7213, 18 U.S.C. § 1030(a)(2)(B), or 18 U.S.C. § 1905,	• Initiate and conduct an employee investigation, if warranted; • Refer to the appropriate USAO; and • Refer to the IRS.

290.7.2 Tax Preparer. If a tax preparer (*i.e.,* certified public accountant, enrolled agent, tax attorney, *etc.*) allegedly violates 26 U.S.C. § 7216:

- Initiate and conduct a non-employee unauthorized disclosure investigation;
- Refer to the appropriate USAO;
- If the preparer is an enrolled agent, also forward a copy of the report to the IRS Employee Conduct and Compliance Office (ECCO). See Section 250.12.1.4, *Reports on Enrolled Tax Practitioners*, and Section 300.8.1, *Referral to Director, Office of Professional Responsibility*, of this chapter for additional guidance; and
- If the preparer is not an enrolled agent, also forward a copy of the report to the IRS ECCO. See Section 250.12.1.5, *Reports on Unenrolled Tax Preparers,* for additional guidance.

290.7.3 State Employee. If a State employee allegedly violates 26 U.S.C. § 7213 or 26 U.S.C. § 7213A concerning return or return information obtained by the State as a result of a Federal-State agreement:

- Initiate and conduct a non-employee UNAX or unauthorized disclosure investigation;
- De-conflict with the Cybercrime Investigations Division which maintains a Safeguards Local Investigative Initiative;
- If the complainant is a State employee responsible for monitoring Federal tax information obtained in a Federal-State agreement, request a copy of an audit trail, training records, warning banners, and official personnel file data to substantiate the allegation;
- Consider working a joint investigation with State authorities, as warranted;
- If a joint investigation is pursued, confirm with State authorities the purpose of the investigation to be criminal or administrative; and
- Refer to the local USAO or State authority, as warranted.

Note: If the return or return information was obtained by the State as a result of a State law requiring the taxpayer to submit a copy of his/her Federal tax return with his/her State return, then the disclosure of the return or return information cannot be prosecuted under 26 U.S.C. § 7213.

The IRS Office of Privacy, Governmental Liaison & Disclosure (PGLD) is responsible for safeguard reviews of:

- State Tax Agencies;
- Child Support Agencies;
- Public Assistance Agencies; and
- Other State and Federal agencies receiving Federal tax information.

The TIGTA Form OI 2076, *Referral Memorandum*, should be annotated in the remarks section advising IRS ECCO to forward an electronic copy of the report of investigation (ROI) to Office of Safeguards at SafeguardReports@irs.gov.

290.8 Investigating UNAX Violations.
If the UNAX allegation warrants an investigation, the Special Agent (SA) will accomplish the following, as appropriate:

- Initiate an investigation using the appropriate UNAX violation code;
- Conduct a preliminary audit trail review utilizing the Data Center Warehouse;
- If necessary, submit a RAF to SDS to request a UNAX analysis to determine if a full UNAX analysis is warranted. SDS will:

    - Conduct the appropriate record checks and UNAX analysis and summarize the results on a Form OI 2028-M, *Memorandum of Interview or Activity*. SDS will notify the SA upon completion of the analysis.

- Review pertinent data obtained from the SDS analysis;
- Interview UNAX victims and suspected UNAX victims, and consider audio recordings where they may be of evidentiary value;
- Interview the subject's supervisor;
- Request and review any IRS Forms 11377, *Taxpayer Data Access*, completed by the subject of the investigation, for investigative leads;
- Complete all other investigative leads on current and former employees, witnesses, and third parties, prior to referral to the USAO for a prosecutorial determination or use of a blanket declination agreement;
- Ensure that all of the above leads are timely documented on the Form OI 6501, *Chronological Case Worksheet*;
- Timely forward the final ROI involving IRS employees to the appropriate IRS office as listed in Section 250.12.1;
- Obtain concurrence from the USAO to forward the ROI pending criminal action;
- Ensure that CRIMES timely and accurately reflects the UNAX source codes, UNAX violation codes, and the resulting criminal and/or administrative disposition codes; and

- If the investigation results in an indictment or information involving a violation of 18 U.S.C. § 1030(a)(2)(B), 26 U.S.C. § 7213, or 26 U.S.C. § 7213A, notify the SAC-Operations Division (OPS). See Section 290.9.1.

290.9 Post Indictment Requirements.
The IRS is required by law to notify victims of unauthorized disclosure or inspection after an indictment or information is filed involving the victim's tax information.

290.9.1 26 U.S.C. § 7431 Notifications. Upon information or indictment under 26 U.S.C. § 7213, 26 U.S.C. § 7213A, or 18 U.S.C. § 1030(a)(2)(B), field personnel will notify the SAC-OPS of the indictment or information via e-mail to the *TIGTA Inv Operations Inbox, and provide the following information:

- Copy of the indictment or information;
- Address of the clerk of court where the indictment/information is filed; and
- Names, Social Security Numbers, and last known address of the taxpayer(s) whose account information is the subject of the indictment/information.

The SAC-OPS will make notification to the IRS PGLD, which will notify the affected taxpayer(s) pursuant to the notification provision in 26 U.S.C. § 7431(e).

290.10 Civil Lawsuits for Unauthorized Disclosures/Inspections.
Under 26 U.S.C. § 7431, a taxpayer may sue the United States if a current or former Federal employee makes an unauthorized disclosure or inspection of return or return information.

290.10.1 Notification of a Lawsuit Under 26 U.S.C. § 7431. If a SA learns that the allegations being investigated are the subject of a pending 26 U.S.C. § 7431 lawsuit, the SA will contact TIGTA Counsel for guidance. TIGTA Counsel will coordinate with OI regarding what actions to take.

DATE: October 1, 2017

CHAPTER 400 – INVESTIGATIONS

(400)-300 Tax Practitioner Investigations

300.1 Overview. The Treasury Inspector General for Tax Administration's (TIGTA) Office of Investigations (OI) investigates complaints of unethical practices against practitioners who represent individuals before the Internal Revenue Service (IRS) and un-enrolled tax return preparers. Practitioner means any individual described in 31 C.F.R. § 10.3.(a-d).

Practitioners are authorized by the IRS to practice or represent taxpayers before the IRS. The regulations governing practitioners are contained in Treasury Department Circular 230, derived from 31 C.F.R. Part 10.

Practitioners include:

- Attorneys
- Certified Public Accountants (CPA)
- Enrolled agents
- Enrolled actuaries
- Appraisers

Un-enrolled tax return preparers have limited rights to represent taxpayers. The rules governing practice of an un-enrolled tax return preparer are set forth in Rev. Proc. 81-38.

This section includes the following information related to Tax Practitioner Investigations:

300.1.1 Acronyms Table.

300.2 Authority. The Inspector General Act of 1978, as amended, grants TIGTA investigative authority and responsibility for tax practitioner investigations.

300.3 Initiating Tax Practitioner Cases. OI initiates Tax Practitioner Investigations:

- On its own initiative;
- At the request of IRS officials; or
- In response to complaints received from IRS employees, taxpayers, and other individuals.

Investigations may be coordinated with appropriate IRS components.

OI investigates complaints against:

- Practitioners and un-enrolled tax return preparers, who attempt to corrupt IRS employees and/or IRS programs that have no employee involvement. See the Memorandum of Understanding between IRS Criminal Investigation (CI) and TIGTA for investigative responsibilities regarding tax return preparers.
- Practitioners and un-enrolled tax return preparers, which also involve alleged misconduct by IRS employees. If an IRS employee is involved, refer to Employee Investigations in Section 280.5.

Plain Talk About Ethics and Conduct (IRS Document 12011), and Treasury Employee Rules of Conduct, 31 C.F.R. § 0.107, require IRS employees to report to TIGTA any alleged criminal misconduct or violation by an IRS employee of Office of Government Ethics (OGE) Standards, Treasury Supplemental Standards, or Treasury Employee Rules of Conduct. This includes, but is not limited to, attempts by a practitioner to corrupt an IRS employee or IRS program. IRS employees must report all other allegations concerning unethical practices by a practitioner or un-enrolled agent through their supervisory channels.

300.4 Information Not Investigated. OI refers complaints or other derogatory information not warranting an investigation to the IRS's Employee Conduct and Compliance Office (ECCO), in accordance with the instructions contained in Section 240.4 and 240.5.

300.5 Coordinating with IRS Components. In any practitioner or un-enrolled tax return preparer investigation involving tax matters being handled or investigated by other IRS components, coordinate the investigation with that office.

300.6 Privacy Act Requirements. Before interviewing the subject of a non-criminal investigation, special agents (SA) will provide and explain Privacy Act Notice 416, Tax Practitioner Interviews, to the subject. SAs will include in the Form OI 2028-M, *Memorandum of Interview or Activity*, documenting the interview of the subject that Privacy Act Notice 416 was provided and explained to the subject.

300.7 Report of Investigation. Prepare reports using the standard format outlined in Section 250.7.

300.8 Referral Procedures. SAs will consider referring information regarding, or the results of, practitioner or un-enrolled tax return preparer investigations to:

- The cognizant office within the IRS;
- United States Attorney's Office (USAO);
- State and local authorities, provided that prosecution has been declined by the USAO and the TIGTA Disclosure Officer has approved the referral; and
- Professional organizations and State licensing authorities. This referral requires approval from the TIGTA Disclosure Officer.

For referrals to State and local authorities, professional organizations and State licensing authorities, see Chapter 700, Chief Counsel, Section 70.5 of the TIGTA Operations Manual for referral procedures.

300.8.1 Referral to Director, Office of Professional Responsibility. In all cases involving practitioners, send a copy of the report, with exhibits, to IRS for referral to Director, Office of Professional Responsibility (OPR) in accordance with instructions contained in Section 250.12.1.4. The original report will be sent to the TIGTA Complaint Management Team (CMT).

If a practitioner is arrested, indicted, convicted, or sentenced, the Special Agent in Charge (SAC) Field Division or SAC Internal Affairs Division (IAD) must provide the following information to the Director, OPR:

- Professional status or title;
- Full name and alias or aliases;
- Date and place of birth;
- Last known home and business address;
- Date and place of arrest, information or indictment, and the ultimate disposition of the case; and
- Copy of the court order of judgment and commitment.

Promptly send a copy of the court order of judgment and commitment to TIGTA CMT to be placed in the original case file.

300.8.1.1 Withholding Notification. The SAC-Field Division or SAC-IAD may withhold notification to the Director, OPR, if the practitioner is not prosecuted, and if the notification could adversely affect current or future investigative actions. Document the justification for this decision on the Chronological Case Worksheet (Form OI 6501).

300.8.2 Referral to Small Business/Self Employed. In cases involving un-enrolled tax return preparers, send a copy of the report to IRS for referral to Small Business/Self Employed in accordance with instructions contained in Section 250.12. The original report will be sent to TIGTA CMT.

300.8.3 Referral to U.S. Attorney. Refer criminal violations to the USAO as described in Section 250.14. If the Assistant United States Attorney (AUSA) gives a prosecutive opinion, send a copy of the report upon request to the AUSA.

300.8.4 Referral to Professional Organizations and Licensing Boards. Referrals to professional organizations and licensing boards require approval from the TIGTA Disclosure Officer. See Chapter 700, Chief Counsel, Section 70.5 of the TIGTA Operations Manual for referral procedures.

If any attorney or accountant, other than a CPA, pleads guilty or is convicted as a result of a TIGTA investigation, the SAC must notify, in writing, the appropriate:

- Professional society
- Disciplinary board
- State licensing or regulatory agency

If a CPA is arrested, indicted, pleads guilty or is convicted as a result of a TIGTA investigation, the SAC must notify, in writing:

American Institute of Certified Public Accountants
The Division of Professional Ethics
220 Leigh Farm Road
Durham, North Carolina 27707

Telephone numbers: (888) 777-7077 or (919) 402-4500

Include a copy of these notifications in the case file.

DATE: April 1, 2020

CHAPTER 400 - INVESTIGATIONS

(400)-310 Federal Tort Claims Investigations

310.1 Overview.
The Office of Investigations (OI) conducts administrative investigations into tort claims arising out of incidents involving TIGTA or Internal Revenue Service (IRS) employees or activities occurring during the course of official business, as applicable. This Section includes information related to investigations of tort claims.

310.1.1 Acronyms Table.

310.2 Definitions.

310.2.1 Tort. For the purposes of this Section, a tort is defined as the negligent or wrongful act or omission, by any TIGTA or IRS employee while acting in the scope of employment that gives rise to injury or harm.

310.2.2 Tort Claim. For the purposes of tort investigations conducted by OI, a tort claim refers to either:

- An administrative claim for compensation filed by, or on behalf of, the party claiming to have suffered injury or damage, with the agency whose employee allegedly caused injury or damage; or
- A suit for damages, filed in U.S. District Court by the party claiming to have suffered injury or damage, against the agency and/or its employee alleged to be responsible.

310.2.3 Federal Tort Claim Act. The Federal Tort Claims Act (FTCA) is a limited waiver of the Federal government's sovereign immunity from certain common law tort claims. With certain exceptions and caveats, the FTCA authorizes plaintiffs to bring civil lawsuits:

1. Against the United States;
2. For money damages;
3. For injury to or loss of property, or personal injury or death;

4. Caused by a Federal employee's negligent or wrongful act or omission;
5. While acting within the scope of their office or employment; and
6. Under circumstances where the United States, if a private person, would be liable to the plaintiff in accordance with the law of the place where the act or omission occurred.

310.2.4 Federal Employee. The term "Federal employee" includes employees of any Federal agency, and persons acting on behalf of a Federal agency in an official capacity, whether with or without compensation. Federal employees not on official duty or acting outside the scope of their employment are considered non-Federal persons for the purpose of this section.

310.3 Purpose of Tort Investigations.
OI conducts tort investigations to establish the facts of potential tort claims, in order to:

- Defend the Government against claims for personal injury, death, or property loss or damage caused by the negligence, wrongful act, or omission of an employee acting within the scope of employment; or
- Aid in the prosecution of Government claims arising from incidents involving TIGTA or IRS employees or activities.

310.4 Criteria for Conducting Tort Investigations.
OI conducts an investigation when:

- Specifically requested by competent authority, including the IRS Office of Chief Counsel (OCC); or
- A non-Federal person suffers personal injury or death resulting from an incident involving TIGTA or IRS activities.

310.4.1 Enforcement Action Deaths or Injuries. OI will not normally conduct tort investigations involving the death of, or injury to, violators or other non-Federal persons that occur during enforcement activities if another law enforcement agency conducts an investigation adequate to protect the Government's interest.

310.4.2 Property Damage. OI does not normally conduct tort investigations in cases solely involving property damage, unless specifically requested by IRS Counsel and IRS Counsel is unable to obtain information from other sources or the TIGTA Designated Torts Claims Official requests assistance. See Chapter 700, Section 100.2.5.1.

310.5 Initiating Tort Investigations.
OI initiates and assigns tort investigations according to their priority and the need to protect the Government's interest. Use the Criminal Results Management System violation code 980-TORT CLAIM.

310.5.1 Initiation Procedures. When an incident occurs, the competent authority requesting the investigation must submit a memorandum and the applicable forms to the relevant TIGTA OI office. The following forms may be applicable:

- Motor Vehicle Accident Report (Standard Form 91);
- Federal Employee's Notice of Traumatic Injury and Claim for Continuation of Pay/Compensation (Form CA-1);
- Statement of Witness (Standard Form 94); and
- Claim for Damage, Injury or Death (Standard Form 95).

310.5.2 Title of Investigation. Title a tort investigation with the location (city and state) and date (month and year) of the incident (*e.g.,* TORT CLAIM RE WASHINGTON, DC accident JAN. 2020). Do not include the name of the involved parties in the investigation title due to Privacy Act restrictions. See Section 310.7 for guidance if employee misconduct is identified during the tort investigation.

310.5.3 Priority of Investigation. It is particularly important to promptly initiate and complete a tort investigation whenever a lawsuit has been filed, or is expected to be filed, against the Government. A lawsuit is likelier to occur in instances that involve the death or serious physical injury of one or more persons.

If the tort investigation involves the death or serious physical injury of one or more persons, the division Special Agent in Charge (SAC) for the area where the incident occurred will immediately initiate the tort investigation and assign the case to an experienced Special Agent (SA).

If the tort investigation does not involve the death or serious physical injury of one or more persons, the SAC will prioritize the tort investigations based on:

- The severity of injuries resulting from the incident;
- Any indications of negligence by Federal employees; and
- The likelihood of future claim(s) for damages.

If the SAC determines an investigation is not warranted, he or she will discuss the matter with the appropriate TIGTA or IRS official.

310.5.4 Notification of Case Initiation. OI will notify the IRS OCC-General Legal Services (GLS) that a tort investigation involving an IRS employee has been initiated. If the tort investigation involves a TIGTA employee, coordination with the SAC-Special Investigations Unit (SIU) is required. The investigating office will notify TIGTA Counsel of the case initiation via the general mailbox at *TIGTA Counsel Office.

310.6 Investigative Procedures.

Review the documents provided by the TIGTA or IRS employee or supervisor when the case is initiated. Secure all available information concerning:

- The circumstances of the incident;
- The duty status of the employee at the time of the incident; and
- The damage or injuries resulting from the incident.

310.6.1 Privacy Act Requirement. As applicable, provide the appropriate Privacy Act notification to the subject of a non-criminal investigation at the beginning of an interview. See Section 210 for additional information.

310.6.2 Circumstances of the Incident. Obtain all information possible about the circumstances of the incident. If available, secure copies of a police report, sketches, and/or other relevant documentation from local law enforcement. If needed, obtain statements from involved parties and witnesses. Refer to Section 310.5.1 for potential forms needed. Ensure that the following are included:

- Police Report:
  - Contains information regarding witnesses and other leads;
  - Shows citations issued; helps determine the party at fault;
  - May include a sketch of the accident scene; and
  - Indicates any physical elements such as weather, road conditions, lighting, etc., which may have contributed to the accident.

- Sketch of motor vehicle accident:
  - Indicate relative positions of all vehicles and pedestrians involved just before and just after collision;
  - Label compass directions, streets, and relevant objects;
  - Indicate measurements; and
  - Show by dotted lines the course followed by each vehicle.

If the police report sketch contains the above elements, an additional sketch is not needed.

310.6.3 Document Pertinent Physical Elements. Document physical elements that contributed to the incident or are at issue, to include weather, road conditions, or lighting. Include any physical changes to the scene since the date of the incident.

310.6.4 Obtain Photographs. Whenever possible and as needed by the investigation, obtain photographs relevant to the incident. Identify the photographs by:

- Date and time the photograph was taken;
- Subject of the photograph;
- Photographer; and
- Case number.

310.6.5 Condition of Involved Vehicles. If relevant, determine if the vehicles involved were in working order at the time of the incident. Inspect vehicle records of any Government-owned vehicles (GOVs) involved in the incident for proper maintenance and servicing.

310.6.6 Determining Duty Status of Employee. An employee is considered to be acting within the scope of his or her employment if the incident occurs while conducting or is related to official business. If the investigation discloses the employee was not acting within the scope of employment, report this information immediately to the SAC. A separate investigation should be initiated to address misconduct issues identified. See Section 310.7.

310.6.7 Determine Damage or Injuries. In investigations of incidents resulting in property damages, personal injuries, or death, document as detailed in Sections 310.6.8-310.6.10 below.

310.6.8 Property Damage and Repairs. In the case of property damage, secure the following information, whenever possible:

- Complete description of damage;
- A professional estimate cost of repairs;
- Any action taken by the responsible party's insurance company or any officials to settle the damages if a non-Federal person is liable for damages to Government property; and
- Photographs of property damage.

310.6.9 Personal Injury and Treatment. If there are injuries, determine the extent of personal injury as soon as possible after the incident. Potential sources of information to verify personal injury may include:

- Hospital records;
- Doctor's records;
- Statements of witnesses;
- Police report regarding first aid or obvious injuries; and
- Records of paramedics or emergency personnel.

310.6.10 Report of Death. If any deaths result from the incident, obtain the following information, whenever possible:

- Exact time and date of death;
- Place of death;
- Immediate cause of death;
- Copy of death certificate; and
- Name, relationship, and address of any persons known to be dependent upon the decedent at time of death (*e.g.,* spouse, children, mentally or physically handicapped family members, etc.).

310.7 Discontinuing Tort Investigations.
Under the following circumstances, a tort investigation will be discontinued before completing all investigative steps:

- The investigation reveals misconduct by the IRS or TIGTA employee; or
- The party at fault admits liability in writing.

310.7.1 Misconduct by Federal Employee. Discontinue the tort investigation when the investigation reveals misconduct by the Federal employee.

- Report the facts relevant to the incident in the tort investigation report of investigation (ROI);

- Initiate and complete an employee investigation concerning the misconduct and report as a separate ROI. Refer to Section 280 of this Chapter for information on conducting IRS employee investigations and Section 330 for information on conducting TIGTA employee investigations; and

- Prepare a cover memorandum when submitting the tort investigation ROI advising IRS OCC-GLS or TIGTA Counsel, as applicable, of the separate employee investigation.

310.7.2 Party at Fault Admits Liability. Discontinue the tort investigation when the party at fault or the insurance company admits liability in writing, and has made, or will make, full settlement.

The SA will notify the Assistant Special Agent in Charge and prepare the ROI including all the information available at the time of discontinuance.

310.7.3 Reporting a Discontinued Investigation. When a tort investigation is discontinued, briefly summarize the reasons for discontinuance in the ROI. Distribute the ROI in the same way as ROIs of completed investigations.

310.8 Report of Investigation.

Prepare the ROI and referral memorandum as outlined in Section 250, *Investigative Reports and Case File Procedures*, of this Chapter.

310.8.1 Distribution of Reports. For IRS employee cases, upload the report to IRS Office of Chief Counsel (OCC) SharePoint site. Annotate the referral memorandum in the remarks section that this is an FTCA investigation and should be forwarded to IRS General Legal Services (CC:GLS:CLP) Attn: IRS FTCA Claims Manager.

For TIGTA employee cases, send the ROI to TIGTA Counsel (*TIGTA Counsel Office). If damage to TIGTA owned/leased property, send one copy of the report to TIGTA's Board of Survey (BOS) Coordinator.

See Section 110 and Chapter 600, Section 130 for reporting incidents involving damage to TIGTA owned/leased Government vehicles and property to the TIGTA BOS.

DATE: July 1, 2019

CHAPTER 400 – INVESTIGATIONS

(400)-320 Proactive Investigative Initiatives

320.1 Overview.
This section contains information regarding the use and development of proactive investigative initiatives for the Office of Investigations (OI), and includes the following:

- Purpose
- Office of Investigations Initiatives Board
- Local Investigative Initiatives
- National Investigative Initiatives
- Investigative Initiative Procedures

320.1.1 Acronyms Table.

320.2 Purpose.
Proactive investigative initiatives are developed to identify potential criminal or administrative violations, which generate investigations that may result in referrals to the Internal Revenue Service (IRS), U.S. Attorney's Office, TIGTA's Office of Audit (OA), or TIGTA's Office of Inspections and Evaluations and in some instances, State and local authorities.

Proactive investigative initiatives include both local investigative initiatives (LIIs) and national investigative initiatives (NIIs). Proactive investigative initiatives are the result of research and investigative intelligence that indicates an operation or procedure is vulnerable to fraud or abuse. A spin-off investigation must be initiated when evidence developed during an LII or NII indicates a potential criminal and/or administrative violation by a named individual.

Special agents are encouraged to seek ways to generate proactive investigations and may find that past successful initiatives offer helpful guidance. Proactive investigative initiatives should not be initiated on individuals who are alleged by a third party to have committed some type of misconduct that would come under the jurisdiction of OI. An investigation should be initiated whenever a named individual has been identified from the initiative.

320.3 Office of Investigations Initiatives Board.
The OI Initiatives Board serves as the approving official for LII initiations for all OI divisions, excluding recurring LIIs and NIIs, which may be approved by the Special Agent in Charge (SAC) of the requesting division. The OI Initiatives Board is comprised of the following members as designated by the Deputy Inspector General for Investigations:

- Deputy Assistant Inspector General for Investigations-Field Operations;
- SAC-Field Division;
- Director, Strategic Data Services (SDS); and
- Assistant Special Agent in Charge-Investigative Support Group, SDS.

The OI Initiatives Board is responsible for identifying and sharing trends with other divisions involved in similar investigative activities and initiatives. The board may also suggest the use of various resources (*e.g.,* SDS Division, Cybercrimes Investigations Division, Criminal Intelligence & Counterterrorism Division, Forensic and Digital Science Laboratory, and OA) to enhance a proposed LII or NII.

320.4 Local Investigative Initiatives.
LIIs may be initiated by any division to probe for potential systemic weaknesses, fraud, abuse, or tax administration vulnerabilities within IRS operations. The objective of an LII is to identify individuals exploiting IRS programs or processes.

320.5 National Investigative Initiatives.
NIIs are initiated when TIGTA has identified a systemic weakness and/or fraud in an LII that has significant national implications to justify expansion to the national level. However, there may be instances in which there is enough indication of a potential systemic weakness to support the initiation of an NII prior to an LII.

320.6 Investigative Initiative Procedures.
LIIs and NIIs are requested and approved through the Criminal Results Management System (CRIMES).

320.6.1 Requesting Approval to Initiate a LII or NII. Both LII and NII proposals are processed and routed to the OI Initiatives Board in CRIMES via an initiative request/task, following the procedures outlined in the CRIMES User Guide.

320.6.2 Initiation of a LII or NII. LIIs and NIIs must be initiated within 10 days of receiving approval by either the OI Initiatives Board or the approving SAC. The date the OI Initiatives Board approves the CRIMES initiative request/task shall serve as the "Allegation Received Date" for the purposes of entering the investigation into CRIMES. For recurring LIIs and NIIs, the SAC approval date will serve as the "Allegation Received Date."

320.6.3 Processing Leads Associated with LIIs and NIIs. Leads generated from LIIs and/or NIIs shall be processed by the receiving division within 60 days. When an investigation is initiated from a lead, the "Allegation Received Date" in CRIMES is the date that sufficient information was obtained to warrant initiating the investigation.

Conduct computer matches for NIIs and LIIs in compliance with the Computer Matching and Privacy Protection Act of 1988 (Computer Matching Act). See Chapter 700, Section 70.8.

320.6.4 Closing LIIs and NIIs. LIIs and NIIs may be closed 180 days after the last spin-off investigation has been referred and all leads are closed. Recurring LIIs and NIIs will be closed at the end of each Fiscal Year.

DATE: April 1, 2019

CHAPTER 400 - INVESTIGATIONS

(400)-330 TIGTA Employee Investigations

330.1 Overview.
The Treasury Inspector General for Tax Administration (TIGTA) expects all employees to meet the highest ethical standards. TIGTA's Internal Affairs Division (IAD) investigates allegations of misconduct by TIGTA employees with the exception of those that fall within the jurisdiction of other agencies, such as the Council of the Inspectors General on Integrity and Efficiency (CIGIE) or Office of Special Counsel.

This section includes the following:

330.1.1 Acronyms Table.

330.2 Reporting Complaints Against Senior TIGTA Managers.
Any complaint alleging impropriety or misconduct by the Inspector General, a Principal Deputy Inspector General, a Deputy Inspector General, the Chief Counsel, the Deputy Chief Counsel, an Assistant Inspector General, or a Deputy Assistant Inspector General, will be reported in writing directly to the Integrity Committee of the Council of the Inspectors General on Integrity and Efficiency via e-mail at: Integrity-Complaint@cigie.gov or in writing to:

CIGIE
Attention: Integrity Committee
1717 H Street NW, Suite 825
Washington, D.C. 20006

More information regarding submitting complaints to CIGIE is available via their website.

Note: Only IAD will enter an intake into the Criminal Results Management System (CRIMES).

330.3 Reporting Complaints Against IAD Employees.
Any complaint alleging impropriety or misconduct by any IAD employee will be reported directly to the Deputy Inspector General for Investigations (DIGI) in accordance with

Chapter 200, Section 60.1.1, of the TIGTA Operations Manual. The DIGI will determine the appropriate course of action, including referral to the appropriate investigative entity, to resolve the allegation(s).

330.4 Reporting Complaints Against All Other TIGTA Employees.
Any complaint alleging impropriety or misconduct by any TIGTA employee not specified in Sections 330.2 and 330.3 will be reported to IAD in accordance with Chapter 200, Section 60.1.1 of the TIGTA Operations Manual.

330.4.1 Complaints Involving TIGTA Employees. The Special Agent in Charge (SAC)-IAD will notify the DIGI and AIGI of all complaints involving TIGTA employees.

330.5 Complaint Processing.
All complaints alleging impropriety or misconduct by any TIGTA employee not specified in Section 330.2 will be the responsibility of IAD. In addition, IAD may conduct, or assist in conducting, such investigations of any TIGTA senior manager at the request or direction of the CIGIE Integrity Committee and/or the Inspector General. Information concerning the CIGIE Integrity Committee can be found at www.ignet.gov.

IAD will not conduct any investigation of its own personnel without the approval of the Inspector General or the DIGI. The approval will be documented on TIGTA Form OI 6501, *Chronological Case Worksheet*.

The SAC-IAD, through the Assistant Special Agent in Charge (ASAC)-IAD, is responsible for ensuring that:

- All allegations of impropriety or misconduct on the part of TIGTA employees are properly investigated;
- Thorough reports of such investigations are prepared;
- Such investigations are referred, if warranted, to the appropriate criminal and/or administrative adjudication authorities; and
- All investigations adhere to appropriate professional investigative standards.

The ASAC is responsible for:

- Directly supervising the special agents (SAs) conducting investigations of impropriety or misconduct pertaining to TIGTA employees;
- Establishing and maintaining working relationships with appropriate criminal and administrative adjudication authorities;
- Maintaining and reporting information regarding the numbers and nature of investigations of TIGTA employees; and
- Recommending, through the SAC-IAD, necessary actions, policies and procedures affecting the integrity of TIGTA.

All investigations of TIGTA employees handled by IAD will be conducted in accordance with the requirements of the TIGTA Operations Manual.

All complainants, witnesses, and subjects of such internal investigations will be afforded the same rights and protections afforded in any other investigation conducted by TIGTA.

TIGTA employees may be required to travel to TIGTA Headquarters or any other alternative posts of duty when being interviewed in an IAD matter. The employee's division will pay for travel expenses related to these interviews.

330.6 Reports of Investigation.
All reports of investigations (ROIs) involving TIGTA employees, conducted by IAD, will adhere to the requirements of the TIGTA Operations Manual. See Section 250.7.

For investigations involving TIGTA SAs, and GS-15 and higher employees that are being referred for prosecution and/or administrative adjudication:

- The ROI will be signed by the ASAC;
- The ROI will be reviewed by the SAC-IAD; and
- The SAC-IAD will sign the referral letter or memorandum and/or Form OI 2076, *Referral Memorandum*.

For investigations involving all other TIGTA employees (GS-14 and below) that are being referred for prosecution and/or administrative adjudication:

- The ROI will be signed by an ASAC;
- The ROI will be reviewed by the SAC-IAD who will determine whether the report will be sent to the DIGI for review; and
- The SAC-IAD will sign the referral letter or memorandum and/or Form OI 2076, *Referral Memorandum*.

330.7 Referral of Criminal Matters to the Department of Justice.
All investigations involving TIGTA employees that substantiate that a Federal criminal law was violated, will be referred to the U.S. Department of Justice (DOJ). The SAs assigned to conduct these investigations will consult with the ASAC to determine the appropriate DOJ component to which the matter will be referred. If the matter under investigation by TIGTA is not a Federal crime, or no evidence supports a violation of Federal law, the SA should not seek, and has no authority to obtain, a declination from DOJ.

Note: Investigations involving substantive tax issues will follow the referral procedures outlined in Section 350.7 of this chapter.

Generally, referrals to DOJ will be made to the appropriate U.S. Attorney's Office for the district in which the offense occurred. Substantiated cases involving TIGTA employees who are not SAs may be presented to intake or duty Assistant U.S. Attorneys (AUSAs).

Substantiated cases involving TIGTA SAs should be presented to the United States Attorney, the First Assistant United States Attorney, or the Chief of the Criminal Division. SAs will not present a case regarding a TIGTA SA to an intake or duty AUSA without the concurrence of the ASAC.

There may be circumstances in which it is more appropriate to refer an investigation to the Criminal Division, Public Integrity Section, or a specific section or division within DOJ. These circumstances may include, but are not limited to:

- Cases in which the reported criminal activity spans more than one judicial district and/or jurisdiction;
- Cases that involve highly specialized matters, such as national security, child exploitation, *etc.*;
- Significant involvement of other Federal law enforcement officers (LEOs) as witnesses or defendants;
- Involvement of DOJ employees, including DOJ attorneys, as witnesses or defendants;
- Involvement of Members of Congress, Federal judges, or senior Federal executives as witnesses or defendants;
- Involvement of public or well-known figures as witnesses or defendants; and
- Cases in which IAD managers determine that it is appropriate to refer the matter to a specific section or division.

IAD will adhere to all other TIGTA policies and procedures when referring investigations to DOJ. If the appropriate DOJ component declines to prosecute an IAD investigation, the SA will document the reasons for the declination on Form OI 2028-M, *Memorandum of Interview or Activity*.

With the concurrence of the DOJ attorney and with the permission of the ASAC, the SA may refer the case to the appropriate State or local prosecutor. Referrals to the State/local prosecutor must follow existing TIGTA policies and procedures. See Chapter 700, Section 70.5, of the TIGTA Operations Manual.

330.8 Referral of Matters for Administrative Adjudication.
The SAC-IAD will establish referral procedures and is responsible for making a referral upon the completion of any investigation of alleged impropriety or misconduct involving TIGTA employees, which will be referred to the second-level manager (or higher) for adjudication.

TIGTA employee tax compliance matters will be referred to an AIGI for adjudication.

In special circumstances, approved by the DIGI or Assistant Inspector General for Investigations (AIGI)-Threat, Agent Safety and Sensitive Investigations Directorate, the DIGI or AIGI can appoint an official from another TIGTA function to review and adjudicate IAD referrals.

This referral will be made after any criminal adjudication is completed. If it is necessary to refer an ROI for administrative action before the completion of criminal prosecution, such referral will only be made with the concurrence of DOJ or State/local prosecutor. The ASAC is responsible for ensuring that such concurrence is documented and that the appropriate TIGTA official is advised of the circumstances involved in the pending criminal prosecution.

DATE: July 1, 2019

CHAPTER 400 – INVESTIGATIONS

(400)-340 IAD-IRS Investigations

340.1 Overview.
Due to their sensitivity, all complaints against senior Internal Revenue Service (IRS) officials, employees of IRS Criminal Investigation (CI), employees of IRS Office of Chief Counsel, and IRS Large Business & International (LB&I) – Assistant Deputy Commissioner (International) personnel in the U.S. or within U.S. Embassies abroad will be investigated by, or the investigation will be conducted under the direction of, the Internal Affairs Division (IAD).

This section includes instructions and procedures for IAD-IRS Investigations concerning the following:

- Primary IRS Investigative Responsibility
- Reporting Complaints Against IRS Officials
- Evaluating Complaints Against IRS Officials
- Investigation of Complaints
- Reports of Investigation
- Referral of Criminal Matters to the Department of Justice
- Referral of Matters for Administrative Adjudication

340.1.1 Acronyms Table.

340.2 Primary IRS Investigative Responsibility.
IAD has the responsibility for investigations of senior IRS officials and IRS LB&I – Assistant Deputy Commissioner (International) employees located in the U.S. and within U.S. Embassies abroad. Additionally, IAD has responsibility for investigations of IRS-CI employees and employees of the IRS Office of Chief Counsel (OCC).

Note: Allegations involving IRS employees located in Puerto Rico and the U.S. Virgin Islands must be referred to the Special Agent in Charge (SAC)-Southern Field Division. Allegations involving IRS employees in Guam or the American Samoa Islands must be referred to the SAC-Western Field Division.

340.2.1 Identification of Senior IRS Officials. Within the IRS, senior officials include:

- Members of the IRS Oversight Board;
- The Commissioner of Internal Revenue;
- The Commissioner's Special Pay Executives; and

- Any IRS official, executive or manager, GM/GS-15 or above, occupying a position within the Senior Executive Service (SES), to include OCC and any IR-1 or IR-3 employees.

340.2.2 Identification of International IRS Personnel. Within the IRS, international personnel shall include employees reporting to the LB&I - Assistant Deputy Commissioner (International), regardless as to geographic location; and all employees assigned outside of the U.S. to include employees assigned to a U.S. Embassy.

340.3 Reporting Complaints Against IRS Officials.
Any complaint alleging impropriety or misconduct on the part of any senior IRS official or IRS LB&I – Assistant Deputy Commissioner (International) employee, received by any Treasury Inspector General for Tax Administration (TIGTA) employee, will be reported to the SAC-IAD.

340.4 Evaluating Complaints Against IRS Officials.
The SAC-IAD or the Assistant Special Agent in Charge (ASAC)-IAD will evaluate each complaint against an employee identified in Section 340.2 to determine an investigative disposition.

In certain circumstances, the SAC-IAD will refer complaints to a field division for evaluation. The receiving SAC will review the complaint and determine whether or not to initiate an investigation.

If the SAC-IAD or an ASAC-IAD determines that an investigation is not warranted and that the complaint is best handled by referring it to the appropriate IRS official, he/she will follow established procedures to refer the complaint to IRS management. See Section 240.1, Section 240.4, and Section 240.5. Prior to referring any complaint or investigation related to employees of the IRS Human Capital Officer, members of the Commissioner's senior staff, and members of the IRS Oversight Board, the SAC-IAD will notify the Assistant Inspector General for Investigations-Threat, Agent Safety, and Sensitive Investigations Directorate.

Note: IAD will maintain oversight and sole responsibility for the disposition of all investigations and complaints involving TIGTA personnel, the IRS Commissioner and their senior staff, all IRS-CI SES personnel, SACs and Directors. IAD will also maintain this responsibility for the IRS Chief and Deputy Chief Counsel, Chief of Appeals and all Commissioners and Deputy Commissioners for the respective business units within the IRS.

Field division SACs will be responsible for the disposition of investigations and complaints involving all other IRS personnel assigned within their areas of operation, including SES, Grade 15 and IR pay banded employees within all IRS Business Units. SACs are not be required to notify IAD when these investigations are initiated; however,

based on the potential sensitivity of the investigations, periodic updates may be requested by IAD.

340.5 Investigation of Complaints.
The SAC-IAD, through the ASAC-IAD, is responsible for ensuring that:

- All allegations of impropriety or misconduct on the part of personnel identified in Section 340.2 are properly investigated;
- Thorough and timely reports of investigations (ROIs) are prepared;
- All investigations are referred to the appropriate criminal and/or administrative adjudication authorities;
- All investigations adhere to appropriate professional investigative standards; and
- Information regarding the number and nature of investigations of such personnel is maintained and reported.

The ASAC-IAD is responsible for:

- Directly supervising the IAD special agents (SAs) conducting investigations of impropriety or misconduct pertaining to personnel identified in Section 340.2;
- Recommending those complaints which can best be resolved through administrative measures without the need for a formal investigation; and
- Establishing and maintaining working relationships with appropriate criminal and administrative adjudication authorities.

In addition, the SAC-IAD may conduct, or assist in conducting, any investigation of the Secretary of the Treasury involving his/her duties as a member of the IRS Oversight Board. Such investigation may be conducted in conjunction with the TIGTA if authorized by Federal disclosure laws.

All investigations of personnel identified in Section 340.2, whether conducted by SAC-IAD or a SAC-Field Division, will be conducted in accordance with all requirements of the TIGTA Operations Manual.

All complainants, witnesses and subjects of such investigations will be afforded the same rights and protections afforded in any other investigation conducted by TIGTA.

340.6 Reports of Investigation.
All ROIs pertaining to investigations of personnel identified in Section 340.2 will adhere to the requirements of Section 250.7. The SAC-IAD will review those ROIs completed by IAD, and the SAC-Field Divisions will review those ROIs completed by field division personnel, to ensure that the ROIs are forwarded to the appropriate authorities.

All ROIs completed by a SAC-Field Division at the request of SAC-IAD, pertaining to investigations of personnel identified in Section 340.2, will receive significant oversight and review by the SAC-Field Division.

For all ROIs pertaining to investigations of personnel identified in Section 340.2, which are being referred for prosecution and/or administrative adjudication:

- The ROI will be reviewed and approved by the assigned ASAC supervising the investigation, and forwarded to assigned SAC for review; and
- The referral letter or memorandum and/or Form OI 2076 will be signed by the assigned SAC.

340.7 Referral of Criminal Matters to the Department of Justice.
All investigations of impropriety or misconduct pertaining to personnel identified in Section 340.2, which disclose evidence of violations of Federal law will be referred to the Department of Justice (DOJ). IAD SAs assigned to conduct these investigations will consult with the ASAC-IAD to determine the appropriate DOJ component to which to refer the matter. Field SAs will consult with their ASAC to determine the appropriate DOJ component to which to refer the matter.

Note: Investigations involving substantive tax issues will follow the referral procedures outlined in Section 280.10.

Generally, referrals to DOJ will be to the appropriate U.S. Attorney's Office (USAO) for the district in which the offense occurred. Cases involving employees who are not IRS-CI SAs may be presented to the intake or duty Assistant U.S. Attorneys (AUSAs). Due to the sensitivity of their position, cases involving IRS-CI SAs should be presented to the U.S. Attorney, the First AUSA, or to the Chief, Criminal Division.

There will be circumstances in which a case may be presented to the Public Integrity Section, DOJ Criminal Division. These circumstances include, but are not limited to:

- Cases in which the reported criminal activity spans more than one judicial district;
- Significant involvement of other Federal law enforcement officers as witnesses or defendants;
- Involvement of DOJ personnel, including DOJ attorneys, as witnesses or defendants;
- Involvement of Members of Congress, Federal judges, or Federal executives as witnesses or defendants;
- Involvement of publicly well-known figures as witnesses or defendants; and

- Cases in which the Inspector General or the Deputy Inspector General for Investigations determine that it is appropriate to refer the matter to the Public Integrity Section.

SAC-IAD will adhere to all other policies and procedures of TIGTA regarding referrals to DOJ in conducting its investigations.

If the appropriate DOJ component declines to prosecute a TIGTA investigation, the SAs will fully document the reasons for the declination.

With the concurrence of the DOJ attorney, and with the permission of the appropriate ASAC, the case SA may refer the case to the appropriate State or local prosecutor for a prosecutive decision. See Chapter 700, Chief Counsel, Section 70.5 of the TIGTA Operations Manual for procedures.

In cases involving senior IRS officials being conducted by a SAC-Field Division, the ASAC-Field Division will consult with the SAC-Field Division prior to referring a case to a State or local prosecutor. All existing TIGTA policies and procedures regarding such referrals will be followed.

340.8 Referral of Matters for Administrative Adjudication.
The SAC-IAD is responsible for establishing referral procedures for all investigations involving senior IRS officials. Upon the completion of any investigation of alleged impropriety or misconduct involving senior IRS officials, and after the review and approval conducted by an ASAC-IAD specified in Section 340.5, the SAC-IAD will refer the ROI to the appropriate IRS official.

The IRS's OCC maintains its own separate personnel and IRS labor relations functions. Upon the completion of any investigation of alleged impropriety or misconduct involving OCC personnel, and after the review and approval conducted by ASAC-IAD specified in Section 340.5, the SAC-IAD will forward the ROI to the OCC's labor relations function.

These referrals will normally be done after any criminal adjudication is completed. If it is necessary to refer an ROI to IRS labor relations before the completion of criminal prosecution, such referrals will only be made with the concurrence of DOJ or State/local prosecutor. The supervising ASAC is responsible for ensuring that these concurrences are fully documented, and that the appropriate IRS labor relations function is advised of the circumstances involved in the pending criminal prosecution.

DATE: October 1, 2017

CHAPTER 400 – INVESTIGATIONS

(400)-350 Department of Justice Tax Division Referrals

350.1 Overview. This section establishes the Office of Investigations (OI) policy and procedures regarding the referral of cases to the Department of Justice Tax Division (DOJ-Tax) and contains the following:

- Department of Justice Tax Division Authority
- Direct Referrals to United States Attorney
- Title 26 U.S.C § 7212(a) Investigations
- Substantive Tax Violations
- Identity Theft Related to Tax Returns
- DOJ-Tax Referral Process and Forms
- Consensual Non-Telephone Monitoring and Search Warrant Requests

350.1.1 Acronyms Table.

350.2 Department of Justice Tax Division Authority. The Department of Justice Tax Division (DOJ-Tax) was created in 1933 in order to provide a uniform and consistent prosecution program with regard to tax laws. Pursuant to 28 C.F.R. § 0.70, the Assistant Attorney General for the Tax Division is responsible for conducting, coordinating, and supervising the prosecution of violations of the internal revenue laws (Title 26).

DOJ-Tax approval is required for any criminal charge where the nature of the underlying conduct arises under the Internal Revenue laws (except for those violations listed in Section 350.3), regardless of the criminal statute(s) proposed to charge the defendant (See DOJ-Tax Directive No. 128).

An offense is considered to arise under the Internal Revenue laws when it involves (1) an attempt to evade a responsibility imposed by the Internal Revenue Code, (2) an obstruction or impairment of the Internal Revenue Service, or (3) an attempt to defraud the Government or others through the use of mechanisms established by the IRS for the filing of Internal Revenue documents or the payment, collection, or refund of taxes. See DOJ-Tax Directive No. 145. TIGTA's external cases typically will fall within the second category (2) above. Employee cases could potentially involve any/all of these factors. See the DOJ-Tax Referral Matrix, Exhibit (400)-350.1, for a snapshot of situations requiring a referral to DOJ-Tax. Flowcharts for additional guidance can be found in Exhibit (400)-350.2 – Non-Employee Cases, and Exhibit (400)-350.3 – Employee Cases.

350.3 Direct Referrals to United States Attorney. DOJ-Tax has authorized direct referral of the following Title 26 violations within TIGTA's jurisdiction to a local U.S. Attorney's office:

- 26 U.S.C. § 7212(a) – Physical assaults, threats of force or violence. Direct referral applies to the first clause of § 7212(a) only. See additional information regarding the "omnibus clause" of § 7212(a) below. See Section 260 of this chapter for Assault/Threat/Interference investigations.
- 26 U.S.C. § 7213 – Unauthorized disclosure of information.
- 26 U.S.C. § 7213A – Unauthorized inspection of return or return information.
- 26 U.S.C. § 7214 – Offenses by officers and employees of the U.S., except tax and financial crime-related employee misconduct. See Section 280.13 of this chapter for tax and financial crime-related employee misconduct.
- 26 U.S.C. § 7216 - Disclosure or use of information by preparers of returns

350.4 Title 26 U.S.C § 7212(a) Investigations. TIGTA's mission and investigative authority includes, in part, investigations of individuals attempting to interfere with the administration of internal revenue laws [Title 26 U.S.C § 7212(a)].

Title 26 U.S.C. § 7212(a) contains two clauses:

1) The first clause prohibits **threats or forcible endeavors** against employees acting pursuant to Title 26 (Interference by threats). An act or threat of force against an IRS employee acting in an official capacity may be prosecuted under the first clause of § 7212(a), which does NOT require DOJ-Tax authorization.

2) The second clause, known as the **"omnibus clause"** of 26 U.S.C. § 7212(a), prohibits any act that **corruptly obstructs or impedes, or endeavors to obstruct or impede**, the due administration of the Internal Revenue Code. A § 7212(a) omnibus clause charge is appropriate for corrupt conduct that is intended to impede IRS activities (*e.g.*, an audit, collection enforcement, or an investigation). Examples of such conduct include, but are not limited to, harassing IRS employees by filing false liens or frivolous documents; providing false information; destroying evidence; or attempting to influence a witness to give false testimony, as related to the IRS activities. See DOJ-Tax Directive No. 129.

   A § 7212(a) omnibus clause charge can also be authorized in appropriate circumstances to prosecute a person who **engaged in large-scale obstructive conduct**, even if it involves the tax liability of others. Examples include, but are not limited to, assisting in preparing or filing a large number of fraudulent returns or other tax forms (*e.g.*,1099-OID), or engaging in other corrupt conduct designed to obstruct the IRS from carrying out its lawful functions.

Cases involving a violation of the "omnibus clause" of 26 U.S.C. § 7212(a) must be referred to the appropriate DOJ-Tax criminal enforcement section for prosecution consideration or to request a tax grand jury.

Some 26 U.S.C. § 7212(a) "omnibus clause" allegations are within TIGTA's area of responsibility (*e.g.*, actions designed to harass IRS employees or broad-based, systemic attempts to interfere with the IRS, such as filing volumes of fraudulent documents in an attempt to hinder or disrupt the IRS systems/processes).

Others are the responsibility of IRS Criminal Investigation (IRS-CI) (*e.g.*, corrupt interference involving tax violations of non-employees, such as refund schemes or filing tax documents/fictitious obligations in an attempt to generate an overpayment). See the Memorandum of Understanding (MOU) between IRS-CI and TIGTA for details of jurisdictional responsibilities.

350.5 Substantive Tax Violations – Coordination with IRS-CI. If an allegation falls within TIGTA's jurisdiction, but also includes the potential for substantive tax violations, request the assistance of IRS-CI in the investigation. A substantive tax violation could generally be defined as a violation wherein monetary damage has been caused, **or attempted to be caused**, to the government through criminal activity involving the Internal Revenue Code. The form these violations typically take are materially false statements on tax forms, willful acts to evade the assessment or payment of a Federal tax, or false claims made to the government via IRS forms.

TIGTA's jurisdiction **generally** does not include refund schemes or tax evasion schemes (**unless an IRS employee is involved**), or fictitious obligations attempting to satisfy a tax debt or induce a refund (**unless impersonation or misuse of Treasury/IRS names/symbols is also present**). These are considered substantive tax violations. Substantive tax violations are investigated by, and processed through, IRS-CI for referral to DOJ-Tax. See the MOU between IRS-CI and TIGTA for further information. Information regarding tax-related employee investigations can be found in Section 280.13.

350.6 Identity Theft Related to Tax Returns. The filing of fraudulent tax returns using stolen identities is within the jurisdiction of IRS-CI. However, there are some variations of IRS-related identity theft that fall within TIGTA's jurisdiction. TIGTA's jurisdiction over identity theft includes the following three areas:

- IRS employee involvement in the identity theft scheme either through unauthorized access, unauthorized disclosure, or as a participant in the criminal activity;

- Preparers who misuse client information or disclose client information to others in furtherance of an identity theft scheme (excluding tax preparers who simply

prepare and file fraudulent tax returns for the purpose of personally stealing refunds); and

- Impersonation of IRS employee(s) in furtherance of the identity theft scheme. (Note: impersonation investigations, absent tax issues, do not require a DOJ-Tax referral.

DOJ-Tax Directive 144 delegates to participating U.S. Attorney's Offices certain authorities for offenses arising from Stolen Identity Refund Fraud (SIRF). The purpose of the delegation is to provide Federal law enforcement officials with the ability to timely address SIRF crimes. The directive authorizes U.S. Attorneys to empanel a tax grand jury, arrest and Federally charge suspects by criminal complaint, and obtain seizure warrants for forfeiture, but the authority is limited and still requires some coordination with DOJ-Tax. See the directive for additional information and specific parameters.

Most instances of SIRF will involve a joint investigation with IRS-CI. Tax preparers who misuse or disclose client information, **without the filing of false returns or thefts of refunds**, may be in violation of 26 U.S.C. § 7216. TIGTA has direct referral authority for this statute. See Section 350.3.

350.7 DOJ-Tax Referral Process and Forms. In a joint investigation with IRS-CI, the TIGTA Report of Investigation (ROI) may be submitted to DOJ-Tax as an inclusion to IRS-CI's report or separately, depending on the circumstances of the case. The appropriate DOJ-Tax Enforcement Division should be contacted for guidance. Separate referrals may be necessary due to the need for a timely submission or other case specific factors. If TIGTA makes a separate referral to DOJ-Tax, ensure the referral states that IRS-CI will be referring its case at a later date. If the referral is made jointly, the responsible SAC will forward the TIGTA ROI to the local IRS-CI SAC for inclusion with IRS-CI's referral to DOJ-Tax.

For information related to each criminal enforcement section, see the DOJ-Tax website at http://www.justice.gov/tax/cessoump1.htm.

350.7.1 TIGTA Referrals to DOJ-Tax. In general, if CI declines to investigate a **tax-related allegation** (employee and non-employee), but there are additional allegations that fall within TIGTA's jurisdiction (*e.g.*, false returns by an IRS employee, false documents filed to harass an IRS employee), TIGTA is required to contact DOJ-Tax to obtain grand jury authorization, authorization for prosecution by the local U.S. Attorney's Office (USAO), or a declination. If CI declines to participate in an investigation, TIGTA does not have the authority for referrals of substantive tax offenses such as 26 U.S.C. §§ 7201, 7202, 7203, and 7206.

If TIGTA disagrees with CI's declination, the ASAC/SAC should elevate the issue to the appropriate DAIGI for further review and consideration, as appropriate. Unresolved

disagreements may be elevated to the AIGI, the DIGI, and ultimately the Inspector General.

350.7.2 DOJ-Tax Prosecution Referral Letter. Utilize TIGTA Form OI 8108, *DOJ-Tax Prosecution Referral*, to refer a completed investigation to DOJ-Tax for prosecution consideration or local USAO authorization. Provide the information as outlined in Form OI 8108 and mail the form letter and the ROI to DOJ-Tax at the address indicated in the form letter. See DOJ-Tax Examples/Referral Letter in the DOJ Tax Library located on the OI webpage. Statute of limitation information can be located at: http://www.justice.gov/tax/readingroom/2001ctm/07ctax.htm.

350.7.3 Referral for Prosecutive Declination on Non-Employee Cases. Utilize TIGTA Form OI 8110-NE, Referral for Prosecutive Declination Non-Employee Subject, when a declination is requested on a non-employee investigation. This form allows for an abbreviated referral to DOJ-Tax when seeking a declination due to a lack of criminal elements or lack of interest by the local USAO, etc. Complete the form per the instructions and mail to DOJ-Tax at the address indicated in Block 1.

350.7.4 Referral for Prosecutive Declination on Employee Cases. Utilize TIGTA Form OI 8110, Referral for Prosecutive Declination and Kalkines Warning Authorization, when a declination is requested on IRS/TIGTA employee tax-related investigations. A DOJ-Tax declination is necessary if the Kalkines Warning is going to be issued in an administrative interview with the subject employee. Complete the form per the instructions and mail to DOJ-Tax at the address indicated in Block 1.

Additional information regarding tax-related and financial investigations of IRS/TIGTA employees can be found in Section 280.13.

350.7.5 Request for Grand Jury Investigation. Utilize TIGTA Form OI 8107, Request for Grand Jury Investigation, to request authorization to empanel a tax grand jury. Provide the information as requested in the form and instructions and mail the form to DOJ-Tax at the address indicated in Block 1 of the form. (See DOJ-Tax Examples/Grand Jury Request in the DOJ Tax Library located on the OI webpage). Exceptions may apply in cases involving Stolen Identity Refund Fraud (SIRF) – see SIRF information above in Section 350.6.

350.8 Referrals to U.S. Attorney's Offices and DOJ-Tax. There could be instances where cases involving both tax violations and non-tax violations are referred separately to a local USAO and to DOJ-Tax. If this occurs, the non-tax violations may be referred to a local USAO, but the SA must advise the AUSA of the tax-related violations and that they require DOJ-Tax review and coordination. After evidence is obtained for the tax-related violations, refer the case to DOJ-Tax for prosecution consideration/authorization utilizing the referral letter (Form 8108) as described above.

350.9 Consensual Non-Telephone Monitoring and Search Warrant Requests. Obtain consensual non-telephone monitoring advice and search warrants for investigations within the jurisdiction of DOJ-Tax through an AUSA at a local USAO. For purposes of gathering evidence in the investigation, DOJ-Tax has authorized contact with a local USAO for these requests; therefore, these requests do not require pre-approval by, or notification to, DOJ-Tax. However, DOJ-Tax retains its authority to prosecute Title 26 violations, and after evidence is obtained from consensual non-telephone monitoring and/or a search warrant, prosecution consideration must be obtained from DOJ-Tax. See Section 350.2 and 350.7 for DOJ-Tax authority and procedures for requesting prosecution consideration.

See Section 170.8 of this chapter for information on consensual non-telephone monitoring procedures.

See Section 140.8 of this chapter for information on search warrants.

https://www.treasury.gov/tigta/foia/efoia-imds/CHAPTER 400 - INVESTIGATIONS

(400)-360 Operations – Inspection Process

360.1 Overview.
This section provides policies and general procedures for the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations (OI) Inspection program and includes the following information:

- Purpose
- Inspection Program Responsibilities
- Inspection Standards
- Inspection Plan
- SAC Certifications/Operational Reviews
- Inspection Team Responsibilities
- SAC/Director Responsibilities

360.1.1 Acronyms Table.

360.2 Purpose.
Legislation, such as the Government Performance and Results Act (GPRA) and the Federal Managers Financial Integrity Act (FMFIA), has changed the management and accountability focus of the Federal government. TIGTA is committed to keeping pace with these changes and providing meaningful investigations, evaluations and other measurements of TIGTA operations and programs.

TIGTA's mission is to prevent and detect fraud, waste and abuse, and to promote economy, efficiency and effectiveness in the administration of TIGTA programs and operations. That mission requires an internal commitment to measure TIGTA's performance and examine the adequacy of internal controls to ensure high quality performance is completed efficiently and effectively.

The purpose of these inspections is to:

- Ensure the quality of the TIGTA investigative products;
- Ensure that TIGTA investigations and administrative operations are conducted in conformance with applicable laws, rules, regulations, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and the TIGTA Operations Manual; and
- Ensure that TIGTA resources are being effectively and efficiently managed.

360.3 Inspection Program Responsibilities.
The Special Agent-in-Charge (SAC)-Operations Division is responsible for conducting inspections of each Field Division office and the various functions at Headquarters,

including, but not limited to, the Technical and Firearms Support Division (TFSD) and the Strategic Data Services (SDS) Division. This program is coordinated through the Assistant Special Agent-in-Charge (ASAC)-Policy Team.

360.4 Inspection Standards.
The CIGIE has developed professional standards and criteria for self-evaluation for Federal Offices of Inspectors General to include investigations. Operations currently utilizes the CIGIE standards to evaluate TIGTA's investigative operations.

Inspections will focus primarily on resource management, investigative results, operational and law enforcement issues and various administrative matters as they relate to the CIGIE Quality Standards for Investigations.

360.5 Inspection Plan.
The Inspection Plan is a process of assurance that ties together annual reporting requirements of TIGTA with the inspection verification and validation process. The process of assurance includes:

- SAC Self-Inspection and Operational Review Certifications (SAC Certifications) submitted by each SAC/Director
- Annual Inventory Reconciliation
- FMFIA Reporting Requirements
- Operations Inspections

360.5.1 Core Areas of Review. There are two core areas of review described below.

- Administrative Core Areas include the following:
    - Physical Security;
    - Vehicles;
    - Oversight of Budget Issues;
    - Inventory and Management of Accountable Property; and
    - Resource Management.
- Investigative Core Areas include the following:
    - Case Management;
    - Evidence and Seized Property Procedures;
    - Grand Jury Procedures;
    - Proper Referral Authorities;
    - Confidential Source and Fictitious Identity Management; and
    - Undercover (UC) Procedures.

360.6 SAC Certifications/Operational Reviews.
Each SAC/Director will submit the following six (6) SAC Certifications:

- Accountable Properties;
- Confidential Sources and Fictitious Identities;
- Space and Physical Security;
- Case Management;
- Evidence and Seized Properties; and
- Resource Management.

The SAC Certifications with attachments should be sent via e-mail to the SAC-Operations Division, with a carbon copy to the ASAC-Policy Team, and uploaded to the SAC Certification SharePoint.

The following SAC Certifications are due on the last day of the month indicated:

- January – Accountable Properties;
- February – Confidential Sources and Fictitious Identities;
- April – Case Management;
- June – Space and Physical Security;
- August – Evidence and Seized Properties; and
- November – Resource Management.

The confidential sources and fictitious identities certification will be conducted in accordance with the Social Security Number (SSN) oversight procedures outlined in Section 180.

The ASAC will conduct the SAC Certifications review for their respective group, identifying the specific issues and any corrective measures taken, if necessary. Each SAC/Director will certify each SAC Certification for their division and also identify and certify that corrective measures, if any, have been completed.

360.7 Inspection Team Responsibilities.
Each division inspection will be conducted by a team of special agents (SAs), headed by a lead from Operations. The remaining members of the inspection team will be comprised of ASACs and Senior Grade 13 SAs from other divisions who have been recommended by their SAC/Director.

The inspections will consist of pre-visitation analysis, onsite visitations resulting in a written report and post visitation analysis.

360.7.1 Pre-visitation Analysis. The pre-visitation analysis generally consists of:

- Quality Case Reviews – by percentage of randomly selected closed cases utilizing the CIGIE Quality Case Review Sheet, results to be included in the GPRA Measures;
- Analysis of the SAC Certifications;
- Briefing with Assistant Inspectors General for Investigation (AIGIs), SAC-Operations Division, the TFSD, and TIGTA Counsel in order to identify any specific division issues; and
- Review of the Division's prior inspection report to ensure issues previously identified have been corrected.

360.7.2 Onsite Visitation. The onsite visitation generally consists of:

- Verification and Validation of SAC Certifications (as determined by the pre-visitation analysis);
- Review of 100% of the evidence;
- Review of Open Cases – 100% review of open cases;
- Review of Complaints - percentage randomly selected, results to be included in the GPRA Measures;
- Interviews of all division employees;
- Verbal briefing with the division SAC/Director; and
- Distribution of a written report, with attachments, containing only findings and best practices.

360.7.3 Post Visitation. The post visitation generally consists of:

- Verbal briefing with the OI Senior Executives; and
- All documentation will be maintained by the Operations Division, ASAC-Policy Team.

360.8 SAC/Director Responsibilities.
The SAC/Director will review the written inspection report and submit a written response, within 15 days, to the items identified for corrective action, as outlined in a memorandum issued by their respective AIGI. A copy of the response will also be submitted to the ASAC-Policy Team.

DATE: July 1, 2020

CHAPTER 400 - INVESTIGATIONS

(400)-370 Cybercrime Investigations

370.1 Overview.
This Section outlines procedures governing the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations (OI) Cybercrime Investigations, and includes the following:

- Cybercrimes
- Cybercrime Investigations Division
- Responsibilities of Cybercrime Personnel
- Consulting with Cybercrimes Investigations Division
- Cyber Investigative Cadre

370.1.1 Acronyms Table.

370.2 Cybercrimes.
Cybercrimes are crimes that use or target computer networks (*e.g.*, the Internet, the Internal Revenue Service (IRS) network, or information systems) as are primarily addressed in the Computer Fraud and Abuse Act of 1986 and enumerated principally in 18 U.S.C. § 1030.

Some specific examples of cybercrimes include, but are not limited to:

- Investigations where the primary offense involves statutes specific to computers and networks by definition, such as 18 U.S.C. § 1030, *Fraud and Related Activity in Connection with Computers*;
- Common offenses under 18 U.S.C. § 1030 include a broad range of illegal activities, such as elevation of privileges to gain access to network resources a user should not access; computer intrusions; unauthorized access of computer files and resources; electronic sabotage or attacks against the IRS network; and trafficking in illicit computer credentials;
- Internet fraud investigations, such as phishing and online impersonation scams;
- Attacks against, or abuse of, public-facing IRS systems (*e.g.*, Get Transcripts); and
- Electronic impersonation (*e.g.*, e-mail, websites) involving IRS resources.

370.3 Cybercrime Investigations Division.
The Cybercrime Investigations Division (CCID) identifies and investigates electronic/computer related crimes or violations that have the potential to compromise IRS systems and networks, and/or corruptly interfere with the IRS' ability to conduct electronic tax administration, both from internal and external threats. CCID is

responsible for conducting and/or evaluating all major cybercrime investigations within OI.

CCID may provide technical and investigative assistance to OI when unique or specific technical issues normally investigated by the CCID are encountered. In these situations, CCID can provide investigative guidance in the following areas:

- Network incident response analysis and investigation;
- Identifying and mitigating external threats to electronic tax administration;
- Assisting Assistant United States Attorneys and special agents (SA) with prosecution of complex c investigations involving computers, networks, and/or applications;
- Preserving electronic evidence “chain of custody;”
- Providing technical advice on obtaining court orders, search warrants, and subpoenas associated with cyber related investigations;
- Supporting joint operations with IRS Computer Security Incident Response Center and Computer Fraud and Analytics Monitoring Team that contain a central point for reporting and analysis, sharing response efforts, and providing investigative support, as appropriate;
- Conducting and assisting with interviews relative to computer/network-related investigations;
- Computer/network vulnerability identification and assessments of IRS applications/systems;
- Recommending preventive, recovery, or mitigation strategies for vulnerabilities and/or attacks, both internal and external;
- Electronic intelligence collection concerning computer/network vulnerabilities;
- Research and development;
- Recommending improvements and system enhancements; and
- Establishing Federal Bureau of Investigation Cyber Task Force contacts and assigned opportunities.

370.4 Responsibilities.
CCID investigative staff are managed by the Special Agent in Charge (SAC)-CCID through Assistant Special Agents in Charge (ASAC)-CCID. CCID investigative personnel are charged with conducting investigations, providing investigative support, managing cyber initiatives, and completing digital extraction and forensic examination support when necessary.

370.4.1 Special Agent in Charge Responsibilities. The SAC-CCID is responsible for formulation and implementation of procedures related to the investigation of OI cyber cases, digital forensics completed by CCID, and management of the Cyber Investigative Cadre (CIC), and other programs within CCID. The SAC-CCID is responsible for the procurement of necessary technical equipment/services for computer related

investigations in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) guidelines, applicable policies, and regulations; and, ensuring the training and certification of all CCID staff. Additionally, the SAC-CCID or his/her designee will determine whether a cybercrime investigation will be initiated; and, if the investigation will be handled by CCID or referred to another division.

370.4.2 Assistant Special Agent in Charge Responsibilities. CCID's ASACs manage the delegation of duties of programs and investigative efforts of the CCID. At the direction of the SAC-CCID, an ASAC-CCID will also evaluate requests and referrals from OI Divisions. An ASAC-CCID will maintain expert knowledge of the requirements in the fields of cybercrimes and forensics; to include legislative changes affecting the profession, and continued familiarity with cyber fields of study (*e.g.*, cybercrime trends, digital forensic, and information technology matters).

370.4.3 Investigative Staff Responsibilities. CCID SAs and other investigative staff are personnel who possess the necessary expertise in computer related fields and technologies. The CCID investigative staff are responsible for identifying new areas for investigation and maintaining cybercrime investigations, pursuing all SAC-CCID directed initiatives, and conducting digital forensic extractions and examinations. The CCID investigative staff will be responsible for conducting digital forensics examinations consistent with the CCID Standard Operating Procedures (SOP), standards established by CIGIE, and the Department of Justice (DOJ). The CCID Staff may assist OI field divisions and the CIC as technical advisors regarding cybercrime and high technology matters.

CCID investigative staff are also expected to maximize their proficiency in the field of digital forensics and information technology, including acquiring specialized training, possessing and developing technical expertise, and maintaining relevant qualifications as assigned by the SAC-CCID or an ASAC-CCID. CCID SAs and other investigative staff are required to maintain professional certifications, as required.

370.5 Consulting with Cybercrime Investigations Division.
Consult with CCID management prior to the initiation of a cybercrime investigation.

CCID may defer cybercrime investigations to the appropriate division on a case-by-case basis. Since electronic evidence is perishable (subject to being deleted or overwritten), discuss potential investigations with CCID as soon as possible.

370.6 Cyber Investigative Cadre.
CIC is a voluntary cadre for SAs interested in pursuing cybercrime investigations within their Division. Other OI investigative staff may be selected for CIC at the discretion of the SAC-CCID. The CIC is a means of leveraging current manpower across OI to address the growing number of criminal investigations involving a cyber-related nexus. The goals of the program are to provide divisions access to cyber tools and computing

resources empowering the CIC to better focus investigative activities, resulting in successful prosecutions of complex investigations. CIC is a cooperative effort between the CCID and other divisions.

370.6.1 Cyber Investigative Cadre Solicitation, Selection, and Training. The SAC-CCID will solicit volunteers and make selections for the CIC based on the needs of the CCID. The application process for CIC will evaluate a CIC applicants aptitude to complete technical trainings through the Integrated Talent Management System, National Cyber-Forensics and Training Alliance, the Federal Law Enforcement Training Center, internal CCID instruction, and other trainings deemed appropriate. Once CIC members are selected and trained, CCID will provide the members equipment and software necessary to sufficiently accomplish an array of cyber investigations.

370.6.2 Cyber Investigative Cadre Activites. CIC membership is a collateral duty.

The CIC activities include, but are not limited to the following:

- Evaluation of referrals to identify and investigate electronic/computer related crimes, or violations that have the potential to compromise IRS systems, networks, and/or corruptly interfere with the IRS' ability to conduct tax administration electronically;
- Provide technical investigative assistance to their respective divisions once appropriately trained; and
- Conduct mobile device and/or computer forensic extractions and examinations in accordance with CCID SOPs, DOJ, and CIGIE guidelines.

See Section 40.8 of this Chapter for additional information regarding collateral duties.

DATE: April 1, 2021

CHAPTER 400 – INVESTIGATIONS

(400)-380 Non-Employee Investigations

380.1 Overview.
This section contains the following information regarding non-employee investigations conducted by the Office of Investigations (OI):

- Case Predication
- Non-Employee Investigation Evaluation Criteria
- Case Initiation Procedures
- Private Debt Collection Contactor Investigations
- Report of Investigation Format

380.1.1 Acronyms Table.

380.2 Case Predication.
A non-employee investigation may relate to allegations against:

- Any person whose identity is known and was not an Internal Revenue Service (IRS) employee at the time the alleged violation was committed;
- Any individual who is contracted by the IRS at the time the alleged violation was committed, such as contract security personnel and employees employed by an authorized Private Collection Agency;
- Any person whose identity is unknown but based on the best information available, is believed to not have been an IRS employee at the time the alleged violation was committed; or
- Business, corporation, or private entity.

380.3 Non-Employee Investigation Evaluation Criteria.
An Assistant Special Agent in Charge or other TIGTA official authorized to initiate investigations must evaluate information received to ensure that it meets the following criteria:

- The nature of the complaint is relevant to the mission of TIGTA; and
- The complaint or information presents one or more logical investigative leads that will either resolve the matter or make it apparent that the matter cannot be further developed or resolved.

380.4 Case Initiation Procedures.
When initiation of a non-employee investigation is warranted, initiate the investigation in the Criminal Results Management System (CRIMES), and ensure that it is titled in accordance with Section 250.

380.5 Private Debt Collection Contractor Investigations.
As part of the IRS's Private Debt Collection (PDC) initiative, delinquent accounts are distributed to approved PDC contractors for collection. The IRS requires the approved PDC contractors to train their employees on all applicable aspects of Section 1203 of the IRS' Restructuring and Reform Act of 1998 (RRA98). PDC contractors are required to comply with all of the provisions of Section 1203. In addition, the PDC contractors are governed by various laws and regulations, including the Fair Debt Collection Practices Act, Public Law 95-109 and Title 15 U.S.C. § 1692 et seq.

The IRS's approved PDC contractors are listed on the *Private Debt Collection Frequently Asked Questions* section of the IRS's website.

When allegations are received, OI will investigate allegations made against PDC contractors that fall within OI's investigative jurisdiction. PDC employees are IRS contractors for OI investigative purposes and will be held to the same investigative criteria as other IRS contractors.

Initiate intakes in CRIMES using the criteria outlined below:

- If the complainant or subject is affiliated with a PDC contractor, a new contact should be created with Employment Status 16 – PRIVATE DEBT COLLECTION EMPLOYEE/AGENCY; and
- If the intake is bridged into an investigation, select Sensitivity Code 18 – PRIVATE DEBT COLLECTION CASE.

380.6 Report of Investigation Format.
Prepare the report of investigation (ROI) in accordance with the instructions in Section 250.7.

Investigations involving IRS contractors are identified on the TIGTA Form OI 2028R, *Report of Investigation* and TIGTA Form OI 2076, *Referral Memorandum*, as an "Employee" case because they are referred to the IRS for adjudication and response, despite being non-employees. When preparing TIGTA Form OI 2076, notate under Section 13, Remarks, "This investigation involves an IRS Contractor, employed by [NAME OF BUSINESS]."

If the case is to be prosecuted in State court, prepare the ROI in accordance with Section 250.7 and send the ROI via CRIMES to the TIGTA Office of Chief Counsel for review prior to referral to the State prosecutor.

DATE: April 1, 2008

CHAPTER 400 – INVESTIGATIONS

(400)-390 Remittance Test Investigations

390.1 Overview.
A Local Investigative Initiative (LII) that probes a potential theft of a taxpayer remittance from an Internal Revenue Service (IRS) office or lockbox facility is also known as a remittance test.

The remittance test program is a continuous proactive activity conducted throughout the year. The purposes of these investigations are as follows:

- To test the various processing systems at IRS Submission Processing Centers, IRS field offices and IRS lockbox facilities to assure that negotiable remittances (e.g., cash, money orders made out in blank, returned refund checks, etc.) are not being fraudulently diverted; and
- To identify any control weaknesses that jeopardize the protection and safeguards over revenues received.

This section includes the following information related to remittance test investigations:

These guidelines are intentionally basic in nature due to the variations in operating practices among IRS Submission Processing Centers, IRS lockbox facilities and IRS field offices. Special Agents (SA) should contact the TIGTA Office of Audit (OA) for reports or information on noted problem areas and control weaknesses disclosed by program reviews of the functional area being tested.

390.1.1 Acronyms Table.

390.2 Remittance Test Initiation Procedures.
TIGTA Office of Investigations (OI) has committed to conducting remittance tests at IRS lockbox banks during the peak filing period of each year. The Special Agent-in-Charge (SAC) is responsible for establishing a test program schedule for remittance tests

conducted at IRS lockbox facilities during other times of the year, and at IRS field offices and Submission Processing Centers. Scheduling of such tests should cover the whole year at different times of peak and non-peak filing periods for each IRS lockbox facility and/or IRS Submission Processing Center within the SAC's jurisdiction. Consideration should be given to conducting tests during different work shifts and in different work units. A remittance test should be random unless there is reasonable suspicion of wrongdoing by a specific IRS or lockbox employee.

A request to initiate a LII remittance test conducted yearly during peak and non-peak filing periods, does not require approval by the Deputy Assistant Inspector General for Investigations (DAIGI) or completion of the TIGTA OI Investigative Initiative Recommendation form. These LII remittance tests are discussed with and approved by the SAC through the Assistant Special Agent-in-Charge (ASAC). The ASAC documents the SAC's approval in the Chronological Case Worksheet (Form OI 6501). All other remittance tests, such as those incorporating new techniques, must be approved in accordance with the procedures in Section 320.4.

Once approved, initiate a LII in the Performance and Results Information System (PARIS) for each remittance test conducted, using the Financial Fraud Profile and violation code 416 - Theft/Embezzlement - Tax Remittance (Lockbox), or violation code 419 - Theft/Embezzlement - Tax Remittance (Non-Lockbox), as applicable. Title the LII using the designation of the IRS Submission Processing Center, IRS lockbox facility or IRS field office being tested. Document the LII as a Master Project Case in PARIS and enter any employee or non-employee spin-off cases initiated as a result of the LII.

390.3 Controlled Remittance Test.
Controlled remittance tests are designed to verify that employees in IRS Submission Processing Centers, IRS field offices and IRS lockbox facilities are not fraudulently diverting negotiable remittances.

390.3.1 Investigative Procedures. In controlled remittance tests, it is generally necessary to enlist the aid of supervisors of the units being tested for introduction, control and recovery of test documents at these facilities. If necessary, notify the appropriate area IRS management official shortly before the test is conducted and advise the official to restrict such information to only those who have a need to know.

Consider the following when planning to conduct a controlled remittance test:

- Choose test documents, such as cash remittances, conscience letters, etc. to fit the particular processing section to be tested;
- Use remittances that are in the form of cash, money orders, or refund checks;
- Discuss prosecutive guidelines for monetary amounts with an Assistant United States Attorney (AUSA);

- Ascertain from IRS management if it would be possible to input test documents into the procedure so they are processed prior to a work break or lunch to maximize the potential to recover evidence;
- Ordinarily, process only one test item through an individual during a test; and
- Consider the use of entity Social Security Numbers (SSN) and/or TIGTA fictitious identities.

See Section 390.9 for information on accounting for confidential expenditures used for remittance tests.

390.4 Uncontrolled Remittance Test.
Uncontrolled remittance tests, sometimes referred to as "blind" tests, are also designed to verify that employees in IRS Submission Processing Centers, IRS field offices and IRS lockbox facilities are not fraudulently diverting negotiable remittances.

390.4.1 Investigative Procedures. If necessary, notify the appropriate area IRS management official shortly before the test is conducted and advise the official to restrict such information to only those who have a need to know. If properly processed, such remittances should eventually post to the Unidentified Remittance File or a fictitious identity account.

Consider the following when planning to conduct an uncontrolled remittance test:

- Determine the dollar amount of the remittance test with the approval of the SAC or designee, but not lower than an ASAC;
- Use odd dollar amounts to aid in identification of the funds in the Unidentified Remittance File; and
- Choose test documents such as a letter with incomplete taxpayer information or a fictitious identity and cash or a blank money order.

See Section 390.9 for information on accounting for confidential expenditures used for remittance tests.

390.4.2 Recovering Funds in the Unidentified Remittance File. After a remittance is posted to the Unidentified Remittance File, the SAC requests reimbursement of the remittance test money using the TIGTA OI Remittance Test Reimbursement Memorandum, and mails the signed memorandum to the IRS Submission Processing Center that services the account.

See Exhibit(400)-280.5 for IRS Submission Processing Center addresses.

390.5 Documentation of Remittance Test.
Prepare a Memorandum of Interview or Activity (Form OI 2028-M) for each remittance test conducted.

Record all denominations and serial numbers of U.S. currency, checks, or money orders used.

The Form OI 2028-M should contain the following:

- The identity of the person(s) tested;
- The IRS Submission Processing Center, IRS lockbox facility or IRS field office, including work units and work shifts tested;
- The identity of IRS or lockbox personnel who assisted; and
- A brief explanation of how the test documents were placed into the work flow and recovered.

390.6 Unrecovered Remittance.
If a remittance is not recovered, consider the following:

- The possibility of innocent error or erroneous handling of the test document; or
- Making arrangements to conduct surveillance of a suspect IRS or lockbox employee or to temporarily detail the employee to another part of the IRS Submission Processing Center, IRS lockbox facility or IRS field office.

390.7 Theft is Suspected.
Establish liaison with the local United States Attorney's Office (USAO) prior to conducting a remittance test to discuss guidelines regarding the use of an ultraviolet light, conducting searches, arrests, etc.

Prior to searching any place or container, the SA should determine whether the employee has a reasonable expectation of privacy (REP) in the area to be searched. If the employee has REP in the area to be searched, the SA needs to obtain a search warrant unless a recognized exception to the search warrant requirement applies (e.g., consent).

Prior to searching the employee, the SA should attempt to obtain consent to search. A consent search of a person who has not been arrested, does not preclude successful prosecution if evidence of a theft is found.

If consent is obtained, conduct the search as directed by the local USAO. A second SA should witness the search.

If the employee does not consent to a search of his or her person, then one cannot be undertaken unless a search warrant is obtained or another recognized exception to the search warrant requirement applies (e.g., search incident to an arrest).

Before any questioning, use another SA as a witness. When there is probable cause to suspect an employee has committed the theft, contact the local USAO for guidance,

and if interviewed, advise the employee of his or her Constitutional right against self-incrimination (i.e., Miranda or Beckwith rights).

If the employee admits to the theft, then:

- Include questioning that covers any other thefts; and
- If advised by the AUSA, obtain an affidavit including a full statement as to advisement of rights, waiver of rights, admission to all elements of each offense identified, and consent to search, as applicable.

390.8 Initiating Spin-Off Investigations.
Initiate an Employee Investigation using the Financial Fraud Profile and violation code 419 - Theft/Embezzlement - Tax Remittance (Non-Lockbox) when a theft occurs and the suspect is an IRS employee.

Initiate a Non-employee Investigation using the Financial Fraud Profile and violation code 416 - Theft/Embezzlement - Tax Remittance (Lockbox) when a theft occurs and the suspect is a lockbox employee.

See Section 280.8.2 for information regarding theft and embezzlement cases.

Include the investigation number in the LII Report of Investigation (Form OI 2028) and enter the employee or non-employee investigation as a spin-off case of the LII in PARIS.

Refer the facts concerning any investigation disclosing a theft to the USAO or an appropriate person in the Department of Justice (DOJ) for a prosecutive opinion. See Section 250.13 for more information on referring cases for criminal action.

390.9 Use of Investigative Imprest Funds in Remittance Test.
Use the investigative imprest fund to obtain money to conduct a remittance test, in accordance with the following procedures:

- For remittance tests initiated by TIGTA, use TIGTA investigative imprest funds, as needed.

- All remittance test expenditures and recovered funds are accounted for using BOC 9103 and Project Code TGTREMITT. See Chapter 600, Mission Support, Section 50.9.6.4 regarding the investigative imprest fund and confidential expenditures.
- Handle as special moneys any test money being held as evidence. Money held as evidence is reported on a Statement of Special Moneys and Property Transaction (Form OI 141) at the time of seizure and is accounted for in the investigative imprest fund as having been expended. See Chapter 600,

Section 50.9.7 of the TIGTA Operations Manual for procedures on receipt and disposal of special moneys and property;

- Any test money not recovered will be accounted for in the investigative imprest fund as having been expended. See Chapter 600, Section 50.9.6.4 of the TIGTA Operations Manual for procedures on accounting for confidential expenditures; and
- Any test money that is recovered will be accounted for in the investigative imprest fund as a recovered confidential expenditure. See Chapter 600, Section 50.9.12.1 of the TIGTA Operations Manual for procedures on accounting for recovered funds.

390.10 Report Format.

Report test results on Form OI 2028 following the instructions in Section 250.7. The Form OI 2028 should contain the following:

- The number of tests conducted;
- The identity of the persons tested;
- The IRS Submission Processing Center, IRS lockbox facility or IRS field office tested;
- The identity of IRS or other personnel who assisted;
- A brief explanation of how the test documents were put into the work flow and recovered; and
- References to any spin-off cases.

Note: It is not necessary to attach copies of IRS documents reviewed. List specific details concerning preparation of documents or remittances on the Form OI 6501.

Forward the Form OI 2028 as instructed in Section 250.12. Send the original Form OI 2028 to TIGTA Records Management and Control.

DATE: July 1, 2020

CHAPTER 400 – INVESTIGATIONS

(400)-400 Theft of Property Type Investigations

400.1 Overview.
This Section includes the following information related to theft of property type investigations:

- Theft of Government Property
- Theft of Non-Government Property
- Investigative Procedures
- Extent of Investigation
- Prosecution in State/Local Jurisdictions

400.1.1 Acronyms Table.

400.2 Theft of Government Property.
The Internal Revenue Service's (IRS) Internal Revenue Manual, Section 10.2.8, *Incident Reporting*, requires that IRS employees promptly report all thefts of Government property to the IRS's Situation Awareness Management Center (SAMC). The SAMC will notify the IRS's local security office and the Treasury Inspector General for Tax Administration (TIGTA) of the incident. Special agents (SA) must ensure IRS employees' have notified the SAMC of theft of Government property incidents.

****
****
****
****
****
**********.

400.2.1 Initiation Procedures – Theft of Government Property. When an investigation is warranted regarding the theft of government property (other than information technology assets or personally identifiable information), initiate an investigation in the Criminal Results Management System (CRIMES) using the "Financial Fraud" violation code 428 - THEFT/EMBEZZLEMENT-IRS FUNDS OR PROPERTY (NON-IT ASSET). See Section 240.

See Chapter 600, Section 130 that outlines reporting lost, damaged or stolen TIGTA-issued personal property.

400.3 Loss or Theft of an Information Technology Asset or Personally Identifiable Information.
In circumstances where a theft or loss involves an information technology asset or personally identifiable information (PII), the CRIMES violation code 529 – LOSS/THEFT IT ASSET (AIRCARD, COMPUTER, SERVER, BLACKBERRY, CELLPHONE, FLASH DRIVE, DVD/CD) must be used.

In circumstances where there is an unknown subject and an intake relates lost or stolen information technology (IT) assets or PII, the intake should be titled according to the loss or theft (*e.g.,* COMPLAINT RE STOLEN LAPTOP).

In circumstances where non-employee intakes are not initiated into investigations, forward the intake to the IRS for information only. "Section 8 – Remarks" of TIGTA Form OI 2070-A, *Complaint Referral Memorandum (Referred for Information Only)* should include, **"Loss/Theft IT Asset-PII. Please forward to Privacy, Governmental Liaison, and Disclosure."**

For non-employee investigations relative to the loss or theft of an IT asset or PII, "Section 13" – Remarks of TIGTA Form OI 2076, *Referral Memorandum* should include **"Please Forward ROI to Privacy, Governmental Liaison, and Disclosure."**

In circumstances where the involvement or negligence of an employee (*e.g.,* IRS employee, contractor, lockbox employee, or private debt collection employee) is determined to be a factor of the loss or theft of an IT asset or PII, a spin-off investigation is required.

400.4 Theft of Non-Government Property.
A theft of non-government property investigation is initiated for a reported theft of personal property, as appropriate. The principal concern in this type investigation is to determine if any IRS employees are involved in such thefts.

400.4.1 Initiation Procedures – Theft of Non-Government Property. When a theft of non-government property type investigation is warranted, initiate an investigation in CRIMES using the violation code 429 - THEFT/EMBEZZLEMENT-NON-IRS FUNDS OR PROPERTY. See Section 240.

400.5 Investigative Procedures.
Consider the following basic steps when conducting a theft of property investigation:

- Identification of the IRS function where the theft occurred;
- Ascertain whether local police or FPS have been notified; if not, have complainant notify the local police or FPS, as appropriate;
- Interview complainant as to the circumstances of the theft;
- Date, time and method of entry;

- Description of damage, if applicable;
- Description, including model and serial numbers, of any property stolen or lost;
- Advise complainant to immediately notify credit card companies, banks, etc., if any of the stolen items could be used to make purchases, withdraw money or write checks in the name of the complainant;
- Advise complainant as to possible hazard of stolen keys for residence and automobile; also consider contacting GSA or building management to change locks on IRS facilities if such keys were stolen;
- Search premises for stolen items hidden for later retrieval, or for items abandoned by the thief as valueless; protect such items for possible fingerprint identification by local authorities;
- Interview any witnesses who may recall any persons in the area of the theft; obtain descriptions of suspects;
- Obtain copies of any “sign-in/sign-out" logs or electronic access logs maintained by building security personnel;
- Obtain and review surveillance video from building if available;
- Obtain the names and titles of any other persons present or with access to the area, such as FPS officials, IRS employees, other Federal, State, or local law enforcement officials, and General Services Administration (GSA) personnel; and
- If the incident involves a burglary or break-in of government owned or leased premises, survey the location for any security weaknesses, and make recommendations to the local IRS security function to correct any deficiencies.

400.6 Extent of Investigation.
Determine the extent of investigation in these cases by the amount of information or number of leads available from the complainant and witnesses. Advise complainants of any significant developments in the investigation and instruct them to report to TIGTA any contact from banks, credit card companies, FPS or local police concerning use or recovery of any stolen items. SAs are responsible for entering lost or stolen Government property valued at more than $500 into the National Crime Information Center through TECS. See Section 150.

When all investigative leads have been addressed and there appears to be no employee involvement, the investigation should be closed. Closing the investigation does not preclude continued cooperation with local authorities investigating the incident.

400.7 Prosecution in State/Local Jurisdictions.
If TIGTA identifies a suspect, contact the TIGTA Office of Chief Counsel before furnishing the information to the local authorities investigating the incident. See Chapter 700, Chief Counsel, Section 70.5.

DATE: April 1, 2021

CHAPTER 400 – INVESTIGATIONS

(400)-410 Criminal Intelligence Program

410.1 Overview.
This section provides guidance relating to the Office of Investigations' (OI) Criminal Intelligence Program (CIP), and includes the following:

- Purpose
- Authority
- Constitutional and Privacy Act Considerations
- Criminal Intelligence Investigation Oversight Guidelines
- Criminal Intelligence Program Responsibilities
- Collecting, Organizing and Maintaining Criminal Intelligence Information
- Criminal Intelligence Investigative Initiatives
- Participation in Joint Terrorism Task Forces
- Coordination with the Federal Bureau of Investigation
- Initiating Investigations on Individuals Identified through Criminal Intelligence Program Local Investigative Initiatives
- Divisional Intelligence Coordinator Activities
- Terrorism Amendments to 26 U.S.C. § 6103
- Foreign Intelligence Activities
- Suspicious Activity Reporting
- Intelligence Advisories
- Threat Categorization

410.1.1 Acronyms Table.

410.1.2 Definitions. The following terms used throughout this section are defined as follows:

Counterterrorism Investigation – Investigations of individuals or groups who seek to further political goals wholly or in part through activities that involve force or violence, or non-violent actions, which have the potential to interfere with the administration of the Internal Revenue laws, and would be in violation of Federal, State, or local criminal laws.

Criminal Intelligence Program – Includes all investigations initiated for the purpose of identifying, investigating, tracking, or deterring criminal activities of individuals or groups who seek to further political goals wholly or in part through activities that involve force or violence, or non-violent actions, which have the potential to impact the safety of Internal Revenue Service (IRS) employees or interfere with the administration of the Internal Revenue laws. This also includes investigations of persons identified through CIP

proactive initiatives who have engaged in activities that would qualify them to be designated as Potentially Dangerous Taxpayers (PDT) or to have a Caution Upon Contact (CAU) indicator placed on the taxpayer's account in the IRS Integrated Data Retrieval System (IDRS).

Intelligence – Information collected by the Treasury Inspector General for Tax Administration (TIGTA) that reasonably indicates criminal activity under the laws of the United States under OI's jurisdiction, which is not associated with any particular ongoing investigation, but could potentially provide the basis for initiation of one or more criminal investigations.

Case Specific Information – Information collected by TIGTA that reasonably indicates criminal activity under the laws of the United States, within OI's jurisdiction, that is associated with an open investigation.

Reasonable Indication – The standard of reasonable indication is substantially lower than probable cause. In determining whether there is a reasonable indication of a violation of law within OI's jurisdiction, the special agent (SA) may take into account any facts and circumstances that a prudent investigator would consider. The standard requires specific facts or circumstances indicating a past, current, or future violation law.

Terrorism – The unlawful use of force or violence, or other non-violent actions (*e.g.*, cyber-attack, bomb attack, active threat) against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

Domestic Terrorism – Violent, criminal acts committed by individuals and/or groups to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature.

The statutory definition of these terms may be found in Title 18, United States Code.

410.2 Purpose.
The purpose of the CIP is to identify individuals and groups that desire to threaten, assault, intimidate, or otherwise impede IRS employees in the performance of their official duties or impede the administration of the Internal Revenue laws.

410.3 Authority.
The Inspector General Act (IG Act), 5 U.S.C. App. 3 § 8D(k)(1)(C), and Treasury Order 115-01 provide that TIGTA shall be responsible for protecting the IRS against external attempts to corrupt or threaten employees of the IRS. Treasury Order 115-01 also authorizes TIGTA to protect the IRS and related entities against internal attempts to corrupt or threaten their employees and facilities and to provide armed escorts to IRS employees when deemed necessary and appropriate.

410.4 Constitutional and Privacy Act Considerations.
CIP investigations raise potential First Amendment constitutional issues related to the exercise of free speech. Therefore, all investigative personnel must be fully cognizant of the Privacy Act requirements regarding First Amendment rights.

The Privacy Act prohibits Federal agencies from maintaining a record describing how an individual exercises rights guaranteed by the First Amendment unless:

- Expressly authorized by statute;
- Authorized by the individual about whom the record is maintained; or
- Pertinent to and within the scope of an authorized law enforcement activity.

Therefore, SAs should not collect or maintain records relating to persons exercising First Amendment rights unless the information is inextricably intertwined with information which indicates such persons and/or groups advocate violence toward IRS personnel or facilities, or advocate activities intended to disrupt orderly IRS operations.

To avoid encroaching on an individual's lawful participation in activities protected by the First Amendment, SAs should:

- Establish that there is a reasonable indication that a group or organization, or a member of a group or organization, poses a threat to IRS employees, operations or facilities;
- Conduct the investigation in the manner least likely to have a chilling effect on an individual's legitimate speech and association;
- Investigate only to the extent necessary to determine whether the group or individual poses a threat;
- Terminate the investigation when it becomes clear that the group or individual poses no threat to IRS employees, operations or facilities; and
- Immediately destroy unsolicited intelligence that may implicate First Amendment rights that is neither mission-related nor within the jurisdiction of another agency. Unsolicited complaint information should continue to be processed in accordance with Section 240 of this Chapter.

Note: Refer relevant threat information to other law enforcement entities, following the procedures set forth in Chapter 700, Section 50.5 and Section 70.5. Coordinate with the Assistant Director (AD), Criminal Intelligence and Counterterrorism Division (CICD).

410.5 Criminal Intelligence Investigation Oversight Guidelines.
CIP investigations are subject to rigorous management review and oversight. Assistant Special Agents in Charge (ASAC) are responsible for reviewing all CIP-related information gathered by OI personnel in their respective groups that is incorporated into cases, proactive investigative initiatives, or OI files to ensure compliance with Privacy Act guidelines. Special Agents in Charge (SAC) shall conduct semiannual reviews of

CIP information gathering activities to ensure compliance with the requirements set forth in this Section.

All CIP local investigative initiatives (LII) shall be initiated in accordance with guidance in Section 320.4. The authority to initiate CIP LIIs may not be re-delegated.

ASAC may authorize preliminary information gathering for the purpose of determining the potential of a CIP LII.

410.5.1 Criminal Intelligence Investigation Factor Test. The following three factors should be considered in determining whether to initiate a CIP-related investigation:

- Is there reason to suspect the group or individual advocate's violence against the IRS specifically?
- Is there reason to suspect the group or individual advocates violence against the Federal government in general, and could such violence potentially have an adverse impact on the safety of IRS employees or facilities?
- Does the group or individual advocate use of non-violent activities against the IRS that are designed to impede IRS employees in the performance of their duties, or to otherwise interfere with the administration of the Internal Revenue laws, *e.g.*, filing false liens or currency transaction reports (IRS Form 8300, *Receipt of Cash Payments Over $10,000 Received in a Trade or Business*)?

If the answer to any of the above three questions is "Yes," a CIP LII may be initiated on a group, or a non-employee investigation may be initiated on an individual.

410.5.2 Determining Membership in Potentially Violent Anti-Tax or Anti-Government Organizations. Individuals closely associated with anti-tax or anti-government groups who promote violence against the IRS or its employees may meet the criteria for a PDT or CAU designation. The mere inclusion of an individual on a membership list or association with a group or organization that promotes violence against the IRS or its employees is not sufficient reason for the IRS to designate that person as a PDT. To meet the criteria for a PDT designation based upon group membership or association, the person must be an "active" member. See Section 260 for specific PDT and CAU criteria.

Use one or more of the following criteria to determine active membership:

- Dues-paying member;
- Officer in the organization;
- Distributes literature on behalf of the organization;
- Makes statements that promote the organization's illegal activities;
- Engages in the planning and direction of the organization's illegal activities; or
- Signs significant documents on behalf of the organization.

If the individual is determined to be a member of, or is closely associated with an anti-tax or anti-government group that promotes violence against the IRS or its employees, consideration should be given to initiating a counterterrorism investigation (LII) on the group to determine if it poses a threat to the safety of IRS employees or facilities and to identify additional members that may meet PDT criteria. See Section 410.5.1 above for criteria to initiate LII on anti-government group.

410.5.3 Information Gathering Guidelines. Criminal intelligence information may only be maintained under authority of an authorized investigation.

SAs should solicit only information that is within the jurisdiction of OI, pursuant to the statutory authority of TIGTA and the authority delegated to TIGTA by the Secretary of the Treasury.

When conducting an approved CIP LII on a group or organization (enterprise), SAs may use any legitimate investigative technique authorized for OI and collect such information as:

- The members of the enterprise and other persons likely to be knowingly acting in furtherance of its criminal objectives, provided that the information concerns such persons' activities on behalf of, or in furtherance of the enterprise;
- The finances of the enterprise;
- Geographical dimensions of the enterprise; and
- Past and future activities and goals of the enterprise.

SAs shall not maintain files containing information about individuals or organizations unless such files are an integral part of a currently assigned case.

When an SA is assigned to and while operating under the authority of a Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF), the SA may solicit any information that falls within the mission and jurisdiction of the JTTF. However, such information may not be maintained in OI files unless that information is to be used as the basis to initiate an OI investigation.

410.6 Criminal Intelligence Program Responsibilities.
TIGTA has established a systematic means by which relevant information is gathered and disseminated and a specific protocol by which this information is organized and maintained. The responsibilities and activities listed below will facilitate the effective collection and dissemination of criminal intelligence information.

410.6.1 Special Agent in Charge-Criminal Intelligence and Counterterrorism Division. The SAC-CICD is responsible for the national coordination and monitoring of CIP activities. This includes the following:

- Liaison/coordination at the headquarters level with other Federal law enforcement agencies;
- Liaison/coordination with IRS headquarters personnel and the IRS Office of Employee Protection (OEP);
- Providing periodic briefings to TIGTA and IRS senior management on status of significant incidents and CIP-related investigations;
- Conducting *ad hoc* studies and analyses relating to CIP as directed by OI management;
- Conducting research of "open source" for information relating to CIP and forwarding such information to the field division as appropriate;
- Monitoring field division initiatives relating to criminal intelligence;
- Preparation of CIP advisories and bulletins;
- Conducting studies and analyses to identify emerging activities of violence prone anti-tax or anti-government groups;
- Developing training and presentations relating to threats and assaults, in coordination with the Operations Division;
- Development and dissemination of policy and procedures regarding CIP activities;
- Validate the data entered to the Criminal Results Management System (CRIMES) relating to the CIP; and
- Participation in the FBI's National JTTF (NJTTF), the FBI's Domestic Terrorism Operation Section (DTOS), and the FBI Washington Field Office JTTF.

Whenever the SAC-CICD, or designee, liaisons with IRS or other Federal law enforcement agencies, any exchange of information shall be consistent with the Privacy Act and 26 U.S.C. § 6103. See Section 410.14 for additional guidance on disclosure of information relating to terrorism.

410.6.2 Criminal Intelligence and Counterterrorism Division Responsibilities. CICD is responsible for the following:

- Managing OI's CIP;
- Providing investigative support;
- Suspicious activity reporting;
- Preparing intelligence advisories;
- Initiating five-year updates on PDTs;
- Administering the Threat Information Notification System (TINS);
- Planning continuity of operations; and
- Overseeing critical or emergency incident coordination.

One or more CICD SAs are assigned to the FBI -NJTTF and the FBI -DTOS, placing them in the role of TIGTA national coordinators for intelligence gathering and sharing. SAs assigned to the FBI task forces/units will develop information that has investigative potential for OI divisions.

CICD will share relevant criminal intelligence information with the Department of the Treasury, as necessary. While OI's statutory focus relates to protecting IRS interests, any threat-related information derived from OI's CIP specifically related to department-wide personnel, facilities and infrastructure will be forwarded to the Department of the Treasury's Office of the Inspector General (TIG) for investigative consideration. As necessary and appropriate, TIG will provide this information to the Treasury Operations Center (TOC) for department-wide dissemination using the TOC's existing information sharing protocols.

410.6.2.1 Requesting Support. Investigative analysts (IA) analyze, process, and distribute strategic, operational, and tactical intelligence related to investigations. This information is provided to the requesting SA through the preparation of Intelligence Analysis Reports (IAR).

IARs are written products specific to a subject, group or other intelligence gap. IAs conduct the necessary research from available sources and provide the information to the requestor in a standard reporting format. The IAR is intended to provide the requesting SA with critical background information and descriptive and actionable intelligence information in support of an open complaint or investigation.

To request an IAR from CICD, SAs must submit a Request Assistance Form (RAF) in CRIMES. IARs should never be included as an exhibit in any investigative case file. TIGTA Form OI 2028-M, *Memorandum of Interview or Activity* may be used to summarize relevant findings from IARs. SAs should independently verify information such as criminal history and warrants upon receiving an IAR from CICD.

Note: RAF's are not required for Level 1 threats or Level 1 incidents. CICD will proactively initiate an IAR and provide immediate analytical support to the OI division responding to the Level 1 threat or incident. See Section 410.17.

410.6.3 Division SAC Responsibilities. The SACs are responsible for the coordination and monitoring of CIP activities at the divisional level. Generally, this will include, but is not limited to, the following:

- Liaison/coordination at the field division level with Federal, State, and local law enforcement agencies within the division that may routinely have or maintain information that would be relevant to the CIP;
- Liaison/coordination with local IRS management officials;
- Participation in local JTTFs or other task forces related to counterterrorism;

- Initiation of LIIs to identify and investigate anti-tax or other anti-government groups operating within the field division whose activities would fall within the jurisdiction of OI;
- Initiation of investigations of individuals suspected of being members of anti-government groups whose activities would fall within the jurisdiction of OI; and
- Coordination with the SAC-CICD on CIP initiatives and significant counterterrorism investigations.

Whenever the SAC, or designee, liaisons with IRS or other Federal, State or local law enforcement agencies, any exchange of information shall be consistent with the Privacy Act and 26 U.S.C. § 6103. See Section 410.14 for additional guidance on disclosure of information relating to terrorism.

410.7 Collecting, Organizing and Maintaining Criminal Intelligence Information. Due to the limited geographical distribution of OI's investigative resources, an effective method of obtaining lead information for criminal intelligence purposes is to leverage, to the extent practicable, the information gathering capabilities of other credible entities, including Federal, State, and local law enforcement organizations, IRS personnel, and open source media.

Criminal intelligence information obtained from these sources must first be evaluated to determine whether it may relate to the OI mission. The information can then be further evaluated to determine if there is a basis to conduct further inquiry or investigation. Generally, the designated Intelligence Coordinator (IC) within the Division where the activities or incident in question occurred or is anticipated to occur will conduct or coordinate this evaluation. Refer to Section 410.13 for CIC duties. Due to the scope of operations of some anti-government groups, this may require coordination with other Divisions or the AD-CICD.

410.7.1 Reliability of Criminal Intelligence Information. Criminal intelligence information, as defined in Section 410.1.2, should be documented on TIGTA Form OI 2028-M, and associated with the CIP LII under which it was obtained. The SA initially receiving the information should also document the reliability of the information. This should be done on the TIGTA Form OI 2028-M in a one-sentence statement, which will be the first paragraph of the narrative.

The reliability of the information will be reported using the following three classifications:

- Extremely Reliable:
  - Previously proven reliable source with corroboration;
  - Information obtained through TIGTA-OI surveillance;
  - Information from official records; or
  - Agrees with other information on individual or group.

- Reliable:
  - Information provided by upstanding citizen who has no personal agenda for providing the information;
  - Previously proven reliable source, but information has not been corroborated; or
  - Agrees somewhat with other information on individual or group.

- Unknown:
  - Reliability of information and source is unknown; or
  - Information is from unreliable source, but, considering other known facts, is possibly true.

Documenting the reliability of information pertains only to intelligence information, not to case specific information as defined in Section 410.1.2.

410.8 Criminal Intelligence Investigative Initiatives.
Criminal intelligence information obtained from the sources cited in Section 410.7, or other sources as appropriate, should be organized and maintained in a manner that permits accurate search capabilities, efficient retrieval, and the ability to conduct thorough analyses.

The foregoing protocols outlined in this subsection should be followed for identifying and collecting criminal intelligence information.

410.8.1 National Investigative Initiative. At the beginning of each fiscal year, the SAC-CICD will initiate a national investigative initiative (NII) from which proactive CIP initiatives will be derived.

410.8.2 Local Investigative Initiative. At the beginning of each fiscal year, each SAC will initiate a reoccurring LII to cover routine or on-going CIP activities conducted within the division by the designated IC or other SAs in the division. This is mandatory for Field Operations and should be initiated by Special Investigations and Support Directorate Divisions, if appropriate. This will include such activities as described in Section 410.13. Division CIP LIIs must be initiated using the "Initiative Request" feature in CRIMES' Workplace and documented as follows:

- Title must be FYXX Criminal Intelligence Program Initiative - Name of Division, for example, "FY21 Criminal Program Initiative - Mid Atlantic Field Division;"
- Type must be "Reoccurring LII;"
- Sensitivity code *8 – Counterterrorism*, is required to be added; and
- Violation code must reflect *63 - Threat Assessment*.

410.8.3 Reports of Investigation for CIP Annual Investigative Initiatives. At the end of each fiscal year, the SAC of the Division shall close the primary CIP LII and prepare a report of investigation (ROI) documenting the results of the division's activities. The ROI shall include:

- A statistical summary of all investigations that may have been initiated as a result of information developed under the umbrella of the annual CIP LII; and
- A summary of significant actions resulting from the division's CIP activities.

The SAC-CICD will close the CIP NII and prepare an ROI containing statistical summaries of the divisions activities as described in the two items above, as well as summaries of any significant activities relating to the CIP program that occurred during the fiscal year.

410.8.4 Other Criminal Intelligence Initiatives. When the a SAC has a need to conduct a more narrowly focused inquiry or activity relating to the CIP, he/she should initiate additional LIIs as necessary. This would include activities such as:

- Investigations of specific anti-tax or other anti-government or terrorist groups operating within the division whose activities come within OI's jurisdiction;
- Participation in task forces, other than JTTF; and
- Participation in other proactive CIP initiatives that are narrow in scope and specific in nature.

Additional LIIs initiated relating to the CIP shall be documented in CRIMES using:

- Sensitivity Code *8 – Counterterrorism*; and
- Violation Code *163 – Threat Assessment*.

When initiating these CIP LIIs, the SAC must follow the case initiation procedures set forth in Section 320.4 of this Chapter. The authority to initiate CIP LIIs may not be re-delegated.

Note: CIP LIIs are not to be initiated on specific, named individuals. At such time as an investigation of a specific individual is warranted, then a non-employee or employee investigation must be initiated as set forth in Section 410.11.

410.9 Participation in Joint Terrorism Task Forces.
At the beginning of each fiscal year, the SAC-CICD shall initiate an NII (NJTTF-NII) from which proactive JTTF initiatives will be derived. The SAC-CICD shall also ensure that a CICD SA is assigned to the NJTTF.

SACs are encouraged to participate in their local FBI-JTTF. Participation in a JTTF provides OI with a means to effectively and efficiently obtain information relating to

groups and individuals that pose a threat to the safety of IRS employees and facilities or who have already committed a criminal act directed against IRS employees or facilities.

SACs may designate, with concurrence from his/her respective Deputy Assistant Inspector General for Investigations (DAIGI) or Assistant Inspector General for Investigations (AIGI), one SA to participate in each of the JTTFs operating within the Division. If a Division has three JTTFs operating within the division, the SAC may designate three SAs to participate, one for each JTTF. A SAC, with concurrence of the FBI supervisory SA supervising the daily activities of the JTTF, will determine the level of participation that each of the designated SAs will have in their respective JTTF assignments.

In accordance with the provisions of the Memorandum of Understanding (MOU) Between the Federal Bureau of Investigation and the Treasury Inspector General for Tax Administration, when participating in a JTTF, the OI SA is authorized to investigate and gather information relating to any matter coming under the JTTF jurisdiction. Because the JTTFs operate under the Attorney General authority, assigned OI SAs must adhere to Attorney General Guidelines while conducting investigations coming under the authority of the JTTF. The FBI issues all guidance on investigative matters handled by the JTTF, including all applicable guidelines and policies. Accordingly, when an SA operates solely under the authority of a JTTF, the SA may not access, disclose, or otherwise utilize tax returns or return information unless the tax returns or return information are accessed and disclosed pursuant to an exception to 26 U.S.C. § 6103. See Section 410.14 for a discussion of the terrorism amendments to 26 U.S.C. § 6103. However, while participating in the JTTF, the OI SA shall endeavor to focus on matters that may be specifically related to the OI mission.

At the beginning of each fiscal year, each SAC will initiate a reoccurring LII to monitor JTTF activities conducted by SAs within their division. This is mandatory for Field Operations and should be initiated by Special Investigations and Support Directorate Divisions, if appropriate. Division JTTF LIIs must be initiated using the "Initiative Request" feature in CRIMES' Workplace and documented as follows:

- Title must be FYXX JTTF Initiative – Name of Division, for example, "FY21 JTTF Initiative Mid Atlantic Field Division;"
- Type must be "Reoccurring LII;"
- Sensitivity Code shall be *8 – Counterterrorism;* and
- Violation Code shall be *163 – Threat Assessment*.

Activity Code 36 must be used by all SAs participating in a JTTF to record time spend on these initiatives in CRIMES Time Management Module.

In accordance with the MOU between TIGTA and the FBI relating to participation in JTTFs, OI will not knowingly act unilaterally on any matter affecting the JTTF without

first coordinating with the FBI. SACs will make all reasonable efforts to refer matters to the JTTF that are logically relevant to the JTTF mission. See Section 410.14 for additional guidance on disclosure of information relating to terrorism.

SACs are encouraged to participate in other counterterrorism- related task forces, with approval of the respective DAIGI or AIGI. However, while participating in such task forces, OI SAs generally may only participate in or conduct investigations that fall within TIGTA's jurisdiction unless the TIGTA has agreed to an MOU regarding OI's participation in such task forces. In such cases, the SAC shall contact the AD-CICD, who shall coordinate with TIGTA-Counsel.

410.9.1 Report of Investigation for JTTF Participation. At the end of each fiscal year, or at such time as OI is no longer participating in a particular JTTF, whichever comes first, the JTTF LII shall be closed and an ROI completed documenting the results of the SA's participation. This will include:

- Significant contributions or information the division provided to the JTTF; and
- A brief summary of all OI investigations that may have been initiated as a result of information developed in the JTTF.

410.10 Coordination with the Federal Bureau of Investigation.
In accordance with 28 C.F.R. § 0.85, the SAC, or his/her designee, shall promptly notify the appropriate JTTF of non-Section 6103 information developed within his/her respective field division that relates directly to a terrorist incident, threat, or activity. If tax returns or return information are to be disclosed, then the SAC shall contact the AD-CICD, who will coordinate with TIGTA Counsel.

Refer to Section 410.14 of this Chapter and Section 50.5.2.6 of Chapter 700 for additional guidance.

410.11 Initiating Investigations on Individuals Identified Through Criminal Intelligence Program Local Investigative Initiatives.
When information is developed through CIP activities that indicates there is a potential that an individual may meet one of the criteria to be designated a PDT, as set forth in Section 260.4.3 of this Chapter, or CAU, as set forth in Section 260.5 of this Chapter, or the individual may have in the past, is currently, or is likely in the future to violate a criminal statute coming under OI's jurisdiction, the individual will be cross-indexed in CRIMES, referencing the CIP LII case number under which the information was initially developed.

When cross-indexing an individual to the CIP LII:

- Use RELATIONSHIP TO SUBJECT code *10 – Other*; and
- Document the REMARKS block of the cross-index section to adequately identify the activities of the suspect individual that are the basis for the cross-indexing.

Appropriate preliminary inquiries should then be made under the LII to determine if there is a **reasonable indication** that the subject would meet the criteria to be designated a PDT/CAU or the subject has committed a criminal violation coming under OI's jurisdiction. In determining the above, the SA must take into account specific facts or circumstances that a prudent investigator would consider.

These preliminary inquiries should generally be limited to the following:

- Law enforcement records checks;
- Interviews of law enforcement personnel;
- Inquiries of other public agencies;
- Obtaining Department of Motor Vehicle photographs of potential subjects for purpose of obtaining or verifying description;
- Interviews of confidential sources;
- TIGTA indices checks;
- Examination of records available to the public and other public sources of information;
- Weapons checks;
- Public statements or writings made by individual;
- Surveillance;
- Use of informants or undercover agents who passively receive information; and
- IRS records checks may only be conducted on persons that advocate activities specifically against IRS employees or facilities, or against the Federal government in general, where such activities could reasonably threaten the safety of IRS employees or facilities, or impede the administration of the Internal Revenue laws. See 26 U.S.C. § 6103(h)(1).

Once these preliminary inquiries have been completed, and a determination is made that there is a reasonable indication the individual would meet the criteria to be designated a PDT/CAU, or has violated a criminal statute coming under OI's jurisdiction, then a spin-off case shall be initiated, and an investigation of the individual's activities conducted, as appropriate. Do not initiate a CIP LII on a specific named individual.

Once the investigation is completed, forward the ROI in accordance with Section 250.7 to the IRS-Office of Employee Protection where a PDT/CAU determination is made, and/or the U.S. Attorney's Office (USAO) in accordance with Section 250.13. Ensure TIGTA Form OI 8273, *Assault, Threat, Threat Assessment, and Harassment Incident Report*, is completed.

In accordance with Section 150.4.3 of this Chapter, on cases referred for PDT/CAU determination, do not provide OEP with information obtained from TECS or the National Crime Information Center (NCIC). TECS or NCIC results may not be provided outside of OI without verification by the originating agency before such a disclosure.

When the spin-off non-employee case is closed, the SAC determines if a review of the ROI by the AD-CICD is warranted to make further distribution of the case (*e.g.*, TIGTA management officials, IRS) If so, then the SAC shall advise the AD-CICD, regarding the closing of the case.

410.12 Divisional Intelligence Coordinator Activities.
Each SAC will designate an SA who will serve as the Divisional IC for all CIP activities. This is mandatory for Field Operations and is recommended for Special Investigations and Support Directorate Divisions, if appropriate. Generally, this will be a collateral duty for the assigned SA, but the SAC may designate it as a full time assignment if the amount of work involved in a particular Division so warrants. Except in unusual situations, the IC should be an SA that is assigned to an ASAC located at the SAC office.

IC activities include, but are not limited to, the following:

- Coordinating intelligence gathering activities on anti-tax, or other anti-government or terrorist groups operating within the field division that may pose a threat to the safety of IRS employees or whose goal is to impede IRS operations through criminal activities;
- Analyzing incident and threat investigation information within the field division to identify emerging trends or significant activities of groups or individuals;
- Liaison and coordination with the AD-CICD on division CIP trends, investigations and intelligence sharing;
- Maintaining liaison with other ICs;
- Conducting routine, periodic liaison with other Federal or State/local law enforcement agencies (especially FBI, Bureau of Alcohol, Tobacco, Firearms and Explosives, and U.S. Marshals Service) to identify individuals or groups that may pose a potential threat to the safety of IRS employees;*
- Conducting routine, periodic liaison with IRS offices within the division to identify individuals or groups that may pose a threat to the safety of IRS employees;* and
- Participating in a local JTTF.*

* These tasks may be completed by other designated SAs within the division.

410.13 Terrorism Amendments to 26 U.S.C. § 6103.
Congress amended 26 U.S.C. § 6103 to address specifically the disclosure of returns and return information in the context of terrorism. Section 402 of the Emergency Economic Stabilization Act of 2008, Pub L. No. 110-343 § 402, 122 Stat 3765, 3835, made these amendments permanent.

Section 6103(i)(3)(B) permits TIGTA, "[u]nder circumstances involving imminent danger of death or physical injury to any individual, ...[to] disclose return information to the extent necessary to apprise appropriate officers or employees of any Federal or State law enforcement agency of such circumstances." While TIGTA SAs may continue to invoke 26 U.S.C. § 6103(i)(3)(B) in terrorism-related situations involving imminent danger of death or physical injury, as counterterrorism investigations become more routine law enforcement activities, SAs may encounter terrorism-related returns or return information in which there is no imminent danger of death or physical injury.

The amendments to § 6103, which address terrorism-related returns or return information in which there is no imminent danger of death or physical injury are summarized below.

The definitions below apply to the following guidance:

- "Taxpayer return information" is return information submitted by or on behalf of the taxpayer to whom the information relates, as distinguished from, for example, information obtained from other sources (*e.g.*, witnesses) during an examination or investigation.
- "Taxpayer identity" means the name of a person with respect to whom a return is filed, the person's mailing address, taxpayer identifying number, or a combination of those items. For purposes of 26 U.S.C. §§ 6103(i)(3)(C), (i)(7)(A), and (i)(7)(B), a taxpayer's identity does not constitute "taxpayer return information."
- "The term 'person' shall be construed to mean and include an individual, a trust, estate, partnership, association, company, or corporation."

410.13.1 TIGTA Initiates Disclosure. TIGTA may initiate a disclosure when it has return information (but not returns or taxpayer return information) related to a terrorist incident, threat, or activity (26 U.S.C. § 6103(i)(3)(C)(i)). The disclosure may be made only to the extent necessary to apprise the head of a Federal law enforcement agency responsible for investigating or responding to the terrorist incident, threat, or activity. The head of the agency may, in turn, disclose that return information to agency employees to the extent necessary to investigate or respond to the terrorist incident, threat, or activity.

TIGTA may disclose to the Attorney General returns or return information (including taxpayer return information) to the extent necessary for, and solely for use in, preparing a request for an ex parte order under 26 U.S.C. § 6103(i)(7)(D). Subsection 6103(i)(7)(D) permits TIGTA to authorize an application for an ex parte order to allow for the disclosure of returns or return information to the head of the appropriate Federal law enforcement agency responsible for investigating or responding to a terrorist incident, threat, or activity. Upon such an ex parte disclosure, the head of the agency, in turn, may disclose the material to agency employees to the extent necessary for them to investigate or respond to the terrorist incident, threat, or activity.

The judge or magistrate may issue an ex parte order if there is reasonable cause to believe, based on information believed to be reliable, that the return or return information may be relevant to a matter relating to a terrorist incident, threat, or activity. If an ex parte order is granted, the designated material shall be solely for use in a Federal investigation, analysis, or proceeding concerning any terrorist incident, threat, or activity.

The following summarizes the above guidance:

TIGTA Initiates Disclosure (§ 6103(i)(3)(C))

Elements (i):

1. TIGTA;
2. May disclose in writing;
3. Return information (not taxpayer return information);
4. Related to terrorism;
5. To the extent necessary; and
6. To apprise the head of an authorized Federal law enforcement agency.

Elements (ii):

1. TIGTA;
2. May disclose in writing;
3. Returns and taxpayer return information;
4. To the Attorney General;
5. To the extent necessary; and
6. Solely for use in preparing an ex parte order.

410.13.2 Another Federal Agency Requests Disclosure. TIGTA may disclose return information (but not returns or taxpayer return information) upon receipt of a written request from the head of any Federal law enforcement agency (or his/her delegate) involved in the response to or investigation of any terrorist incident, threat, or activity. The written request must set forth the specific reason/reasons why the disclosure may be relevant to a terrorist incident, threat, or activity. TIGTA may disclose the material to employees of any Federal law enforcement agency who are personally and directly

engaged in the response to or investigation of any terrorist incident, threat, or activity. They, in turn, may only use the return information for the terrorist response or investigation.

The head of the Federal law enforcement agency receiving the disclosure may, in turn, disclose that material to employees of any State or local law enforcement agency if that agency is part of a team with the Federal law enforcement agency in responding to or investigating a terrorist incident, threat, or activity. The return information may only be disclosed to State or local law enforcement agency employees who are personally and directly engaged in that response or investigation.

TIGTA may also disclose return information (but not returns or taxpayer return information) upon receipt of a written request from an employee of either Department of Justice (DOJ) or the Department of the Treasury who was appointed by the President with the advice and consent of the Senate, or from the Director of the U.S. Secret Service (USSS), provided that the employee is responsible for the collection and analysis of intelligence and counterintelligence information concerning any terrorist incident, threat, or activity. The written request must set forth the specific reason(s) why the disclosure may be relevant to a terrorist incident, threat, or activity. The material may be disclosed to employees of DOJ, the Department of the Treasury and other Federal intelligence agencies who are personally and directly engaged in the collection or analysis of intelligence and counterintelligence information or an investigation concerning any terrorist incident, threat, or activity. They, in turn, may use the return information only for the terrorism-related collection, analysis, or investigation.

The following summarizes the above guidance:

Federal Agency Requests Disclosure § 6103(i)(7)

Elements (A)(i):

1. If an authorized law enforcement officer
2. makes a written request specifying why a disclosure may be relevant to terrorism
3. TIGTA
4. may disclose
5. return information (not taxpayer return information)
6. to employees of a Federal law enforcement agency
7. personally and directly engaged in the response to or investigation of terrorism.

Elements (A)(ii):

1. The head of a Federal law enforcement agency
2. who obtains return information under (A)(i)
3. may disclose that return info

4. to State or local law enforcement officers
5. personally and directly engaged as part of a team with the Federal law enforcement agency in a terrorism response or investigation.

Information disclosed under (A) may only be used for the particular response or investigation for which disclosed.

Elements (B):

1. If an authorized DOJ or Department of the Treasury official, or the USSS director
2. responsible for collecting and analyzing terrorism intelligence and counterintelligence information
3. makes a written request specifying why a disclosure may be relevant to Terrorism
5. TIGTA
6. may disclose
7. return information (not taxpayer return information)
8. to the requestor, and to Federal intelligence agency employees personally and directly engaged in collecting or analyzing terrorism intelligence and counterintelligence information or investigating terrorism.
9. The information disclosed may only be used for that terrorism work.

410.13.3 Expansion of Provisions Concerning Ex Parte Orders. The legislation expands the circumstances in which an ex parte order may be granted. Under 26 U.S.C. § 6103(i)(7)(C), the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, or any United States Attorney may authorize an application to a Federal district court judge or magistrate for an ex parte order. The judge or magistrate may grant an ex parte order if there is reasonable cause to believe, based on information believed to be reliable, that the return or return information may be relevant to a matter relating to a terrorist incident, threat, or activity, and if the return or return information is sought exclusively for use in a Federal investigation, analysis, or proceeding concerning any terrorist incident, threat, or activity.

The ex parte order may provide that returns or return information be open to inspection by, or disclosure to, any Federal law enforcement or intelligence agency employees who are personally and directly engaged in any investigation, response to, or analysis of, intelligence and counterintelligence information concerning any terrorist incident, threat, or activity. Those employees may use the returns or return information solely in the investigation, response, or analysis, and in any judicial, administrative, or grand jury proceedings, pertaining to the terrorist incident, threat, or activity.

The following summarizes the above guidance:

- Subsection 6103(i)(7)(C) expands the availability of ex parte orders to disclose returns/return information to Federal law enforcement agency and Federal intelligence agency employees personally and directly engaged in terrorism intelligence and counterintelligence work.
- Application for the ex parte order must give reasonable cause to believe that the disclosure may be relevant to a matter relating to terrorism. The material must be sought exclusively for use in Federal terrorism work.

410.14 Foreign Intelligence Activities.
Foreign intelligence information is distinct from criminal intelligence and primarily comprises information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents, which is essential to the national security of the United States. Foreign intelligence activities by Federal agencies are governed by Executive Order (EO) 12333 (as amended), which provides for the effective conduct of United States intelligence activities and the protection of constitutional rights. EO 12333 generally identifies the goals, direction, duties and responsibilities of the national intelligence effort and specifies the conduct of foreign intelligence activities.

Although the IRS does not engage in foreign intelligence activities, TIGTA SAs should be familiar with EO 12333 and Section 8.a(5) of Treasury Order 115-01, which requires all employees of the Department of the Treasury to promptly and directly report to TIGTA any information regarding possible improper or illegal foreign intelligence-related activities of United States intelligence agencies, if that conduct is related to the IRS. TIGTA field personnel will promptly report any information regarding these matters to CICD for evaluation and further guidance.

If authorized by 26 U.S.C. § 6103, SAs should refer, through CICD, any information related to international terrorism or espionage promptly to the FBI. In addition, SAs should immediately notify CICD, who will then notify the respective DAIGI or AIGI of any information related to international terrorism or espionage that may impact the safety of IRS employees. This information will be evaluated and forwarded to the appropriate authorities.

410.15 Suspicious Activity Reporting.
For the purposes of OI policy, “suspicious activity” is any behavior that is indicative of criminal activities or other pre-operational planning related to a security threat to any IRS office/building/facility, TIGTA office, other Federal building or public location.

410.15.1 Nationwide Suspicious Activity Reporting Initiative. The Department of Homeland Security and DOJ Nationwide Suspicious Activity Reporting (SAR) Initiative provides law enforcement and security agencies with tools to assist in establishing

investigative links in the course of combating crime and terrorism by creating a national capacity for the gathering, documenting, processing, analyzing, and sharing of SAR information in a manner that rigorously protects the privacy, civil rights, and civil liberties of Americans. Subsequently, all Federal law enforcement agencies are mandated to participate in the initiative.

Any OI employee who observes, or is informed of, any articulable activity that may reasonably be considered suspicious will immediately report the suspicious activity, providing as much detail as possible, to CICD by telephone or via email. Two types of information can be reported: 1) non-TIGTA and non-IRS related information and 2) TIGTA and IRS-related information. Upon receipt of the information, CICD will enter a suspicious activity report into eGuardian or Guardian if disclosure is permitted under 26 U.S.C. § 6103 and/or the Privacy Act. Entries into eGuardian and Guardian are only authorized by CICD personnel.

See Section 400-70 for authorized disclosures. Contact the Disclosure Branch of the Office of Chief Counsel for guidance. CICD will make the appropriate notifications to affected headquarters and/or field divisions, if warranted.

410.15.2 Emergency Circumstances. In circumstances where an imminent danger of death or physical injury to any individual exists, OImay disclose return information to the extent necessary to apprise the appropriate Federal or State law enforcement agency of such circumstances. See 26 U.S.C. § 6103(i)(3)(C). If a disclosure of return information is made, an accounting of the disclosure must be maintained. See Chapter 700, Section 50.7. 3.

410.16 Intelligence Advisories.
Intelligence advisories alert TIGTA and IRS management officials to significant activities of anti-government groups or individuals that may affect the safety of IRS personnel and facilities and OI personnel and IRS management officials of current terrorism-related information and trends.

Because CICD advisories may contain information that is protected from disclosure under 26 U.S.C. § 6103 and/or the Privacy Act, an OI manager must authorize the release of a CICD intelligence advisory outside of TIGTA. See Section 70 for authorized disclosures. Contact the Disclosure Branch of the Office of Chief Counsel for guidance.

410.17 Threat Categorization.
To effectively categorize and appropriately respond to threats against IRS personnel, facilities, and infrastructure, CICD developed a four-level hierarchy to quickly triage threats.

The four levels are described as:

- LEVEL 1. This level encompasses situations involving a direct threat of an imminent physical assault against identifiable IRS personnel (in relation to a known or implied nexus to their employment), facilities, or infrastructure. Additionally, sensitivity factors apply if the threat was made concerning the IRS Commissioner, a member of the Commissioner's immediate staff, any IRS Business Unit Commissioner, or if the threat significantly impacted the operations of another government agency co-located in or near an IRS facility. A sample Level 1 threat is:

  "I have a gun and I am going to the IRS office to kill everyone there."

  Powder mailings, bomb threats, or other threat related incidents, such as protests, law enforcement events, deviation from normal operations related to weather or mechanical issues (*e.g.*, heating or cooling issues, or no power) which cause the IRS to divert from normal operations, or cause significant personnel or operational disruptions, would also fall into this category.

  A Level 1 threat demands an urgent response by OI. CICD is responsible for making a determination as to what is considered a Level 1. CICD will consult with the appropriate SAC and ASAC to determine if mitigating factors exist.

  A Level 1 Expedited notification utilizes the TINS program (see Section 410.18.1) when factors exist that require the IRS Commissioner to be directly advised, such as the death of an IRS employee in the performance of their official duties.

- LEVEL 2. This level encompasses indirect or less specific threats against IRS personnel, facilities, or infrastructure. These are generally not imminent threats, but rather conditional statements made about some potential, future triggering action. Threats in this category may also involve individuals who lack the apparent physical ability to carry out a specific threat. A sample Level 2 threat is:

  "If I don't get my refund soon, someone might get hurt."

- LEVEL 3. This level encompasses activities or efforts to intimidate/harass IRS employees or to obstruct IRS operations by way of "paper terrorism" or other harassing actions. A sample Level 3 threat is:

  A subject who filed false IRS income documents or Uniform Commercial Code-1 financial instruments against IRS, judicial, or other Government employees due to their official capacity/duties.

- LEVEL 4. This level encompasses threat assessments and situations where individuals make general statements advocating assaults or hostilities against

IRS personnel, facilities, or infrastructure. Preliminary reports of threats lacking sufficient detailed information will initially fall into this category unless more information is developed to elevate the threat to a higher category. Information relative to threats of suicide without any additional statements related to harming an IRS employee or facility should also be considered in this level. A sample Level 4 threat is:

"These taxes drive me nuts, I should just commit suicide."

410.17.1 Threat Information Notification System. The TINS was created to streamline threat information between OI and IRS security personnel. The timely and accurate relay of threat information will allow the IRS to take the appropriate action, such as extending the security perimeter, shutting down operations, or raising the alertness level at the affected IRS locations.

Whenever a complaint with the following violation codes is entered into CRIMES, a CRIMES Post-it is sent to CICD:

101 - Threat (Non-IRS employee subject);

110 - Physical Assault (Non-IRS employee subject);

141 - Bomb Threat;

142 - Bomb/Incendiary Device;

144 - Biological/Chemical Substance; or

161 - Workplace Violence (IRS employee subject).

These automated notifications initiate a CICD process regarding the subject of a **Level 1 threat only**, in which a CICD intelligence analyst will query numerous Federal, State, military, other intelligence databases, as well as a variety of open source databases regarding the subject. The results of this research will be forwarded to the responsible SAC, ASAC, and SA.

Additionally, the CICD IA will produce a *Level 1 Threat/Incident Notification* and forward it, via e-mail, to OI Executives and IRS stakeholders via the IRS Threat Information and Critical Incident Response Center (TIRC). The TIRC consists of senior members of all IRS business units, to include the IRS Facilities Management and Security Services (FMSS), the Office of Online Fraud Detection and Prevention, IRS Criminal Investigation, and the Computer Security Incident Response Center.

CICD tracks Level 1 threats and incidents and will provide substantive updates or a final report to the TIRC with information obtained from OI field management and its own research. The final TINS will include the following:

- Whether or not the subject has been located and interviewed;
- Disposition (mindset) of subject, based upon the interview;
- Subject's statement regarding use of weapon, bomb, or incendiary device referenced in threat;
- Brief synopsis of additional investigative details; and
- Statement regarding subject's intentions, based upon the interview.

410.17.1.1 Level 1 Threats and Incidents. Threat information that is categorized as a Level 1 threat or Level 1 incident is to be immediately addressed by the responsible OI division and CICD personnel until it has been mitigated and determined to no longer meet the Level 1 threat criteria. This is better accomplished through the real-time intelligence support by CICD and through coordination with the affected divisions' SACs and ASACs.

410.17.1.2 Non-Level 1 Threats and Incidents. When threat information is received by CICD that is not categorized as a Level 1 threat or Level 1 incident but still has the potential to affect the operations of the IRS, CICD uses one of four other TINS notifications to advise the necessary stakeholders of those incidents or events:

- IRS Related Incidents;
- IRS Related Events;
- Non-IRS Related Incident; and
- Non-IRS Related Events.

An incident is defined as something that is happening, or has already happened; a distinct action, or an episode. Incidents always require a response from either security personnel, law enforcement personnel, or both.

An event is defined as something that is anticipated, such as a demonstration, a VIP visit, etc. It is something that occurs in a certain place during a particular interval of time. An event notification is made for situational awareness and may not require a security or law enforcement response.

410.17.2 The 20/20 Response Protocol. To strengthen the TINS process, CICD utilizes the "20/20 Response Protocol" to ensure that the appropriate stakeholders receive relevant and timely information to make key decisions within their functional areas.

Upon receiving an actionable Level 1 threat or incident notification, the affected SAC, ASAC, and the IRS, FMSS office have 20 minutes to acknowledge receipt by replying back to CICD. If after 20 minutes no response has been received, CICD will attempt to contact by telephone the recipients who did not respond. If no one can be reached after a total of 40 minutes following TINS dissemination, CICD will attempt to contact

the message recipient's functional executive to ensure that the alert receives the proper attention. This protocol does not apply to IRS and non-IRS related event and incident notifications. Those notifications are for informational purposes and no acknowledgement of receipt is required.

DATE: April 1, 2016

CHAPTER 400 - INVESTIGATIONS

(400)- 420 Foreign Language Award Program

420.1 Overview.
This section establishes TIGTA policy and procedures for granting cash awards to law enforcement officers who possess and make substantial use of one or more foreign languages in the performance of their official duties.

This section contains information regarding:

- Authorities
- Definitions
- Qualifying Foreign Languages
- Foreign Language Capability
- Foreign Language Proficiency Testing
- Eligibility Requirements
- Cash Award Amounts
- Employee Responsibilities
- Manager Responsibilities
- Approving Official Responsibilities
- Reconsideration Procedures
- Program Timetable

420.1.1 Acronyms Table.

420.2 Authorities.
The following authorities authorize payment of a cash award and establish policy and procedures for granting a cash award to law enforcement officers who possess and substantially use one or more foreign languages in the performance of official duties:

- 5 U.S.C. §§ 4521- 4523
- Treasury Personnel Manual, Chapter 451.1

420.3 Definitions.
The following are definitions of terms used in the application of the TIGTA Foreign Language Award Program (FLAP).

Law Enforcement Officer – a law enforcement officer as defined by 5 U.S.C. § 8331(20) and 5 U.S.C. § 8401(17). TIGTA employees eligible for this award are employees in the ES/GS-1811 series.

Basic Pay – the rate of pay fixed by law or administrative action for the position held by an employee before deductions and exclusive of additional pay of any kind. Basic pay **does not** include:

- Overtime pay - scheduled or administratively uncontrollable
- Law Enforcement Availability Pay (LEAP)
- Sunday or holiday pay
- Night differential
- Post differentials or cost of living allowances
- Interim geographic adjustments
- Special pay adjustments for law enforcement officers in selected cities under § 404 of the Federal Law Enforcement Reform Act of 1990, 5 U.S.C. § 5305, note.
- Locality-based comparability payments for GS employees in locality pay areas

Basic pay **does** include the higher minimum rates for law enforcement officers under § 403 of the Federal Law Enforcement Reform Act of 1990, 5 U.S.C. § 5305, note and the special salary rates.

The foreign language cash award is computed on a Special Agent's (SA) basic pay in effect during the last pay period of the calendar year in which the SA's foreign language use is being reviewed. The cash award is considered part of a SA's annual aggregate pay and therefore is subject to a limitation. Specifically, total aggregate pay cannot exceed the annual rate of basic pay for Level V of the Executive Schedule for any calendar year.

The cash award is in addition to basic pay and does not increase a SA's base salary for purposes of retirement or life insurance. The cash award is subject to income tax withholding.

Possesses a Foreign Language – achieving a specified speaking skill level using the Federal Interagency Language Roundtable (FILR) proficiency testing and rating system. To be eligible for an award under the FLAP, a SA must possess a minimum proficiency rating of S-2 or above. See Section 420.6.2 for proficiency ratings.

Substantial Use – the usage of one or more foreign languages in the performance of official duties for at least 10 percent of the scheduled duty hours in a calendar year.

For **full-time** SAs**,** substantial use equates to 209 hours or more of foreign language use while performing official duties (e.g., 10 percent of a 2087-hour work year). Use of a foreign language during LEAP hours worked in the same calendar year are included in the computation for substantial use.

For **part-time** SAs**,** substantial use is determined by calculating the percentage of a 40-hour week that a SA is scheduled to work, and multiplying that percentage by 209 hours (the minimum number of hours a full-time SA would have to use a foreign language in order to meet the substantial use requirement).

> For example, a SA scheduled to work 24 hours per week would have to use a foreign language for 125 hours during the calendar year (24/40 = 60%, 209 x .60 = 125.4 or 125 hours).

A SA who does not meet the full-time or prorated part-time substantial use requirements may not be considered for an award under the FLAP. If a SA meets these requirements while using a foreign language for official duties for only a portion of the award year (e.g., 6 months or 9 months as a result of retiring or resigning), the amount of the award will be prorated based on that portion of the calendar year that the foreign language was used in the performance of official duties.

A SA who does not meet the requirements for a foreign language award (*e.g.*, incidents of one-time or short term use) may be considered for a Special Act Award. See Chapter 600, Section 70.33.5.3 of the TIGTA Operations Manual for award guidelines.

Official Duties – normally relate to the duties and responsibilities described in a SA's position description. Examples include, but are not limited to, the following:

- Teaching;
- Speaking;
- Reading;
- Writing;
- Surveillance;
- Protection assignments;
- Conducting or being a witness to an interview; and
- Official public relations work.

Hours spent learning a foreign language, attending class as a student, or taking the proficiency test to participate in the FLAP are not official duties for the purpose of qualifying for an award in the FLAP.

The Deputy Inspector General for Investigations (DIGI) makes the final decision on what constitutes use of a foreign language in the performance of official duties.

420.4 Qualifying Foreign Languages.
Foreign languages that qualify for the FLAP are those recognized as a method of speech and communication by the FILR and are generally not restricted.

Sign language where a foreign language is not involved does not qualify for the FLAP. Where English is not the primary language used in performing the SA's official duties, substantial use of English does not qualify for the FLAP. For example, if Spanish is the primary language used in performing official duties and a SA speaks English only occasionally during the performance of his/her responsibilities, the SA cannot receive an award for use of the English language under the FLAP. Additionally, using a foreign language as a matter of personal preference rather than as a work requirement does not qualify for an award.

The DIGI makes the final decision on whether the use of a foreign language in the performance of official duties qualifies for the FLAP.

420.5 Foreign Language Capability.
A SA applying for the FLAP must report their foreign language capability to his/her Special Agent in Charge (SAC) through their Assistant Special Agent in Charge (ASAC). The SA must complete a Foreign Language Award Program Application (Form OI 9731) indicating each language for which the SA wishes to be tested and recognized, as well as a brief self-assessment of the estimated proficiency level for each foreign language identified. The abbreviated descriptions of the foreign language proficiency levels attached to the application may be used as a guide for writing the self-assessment or the SA may identify the speaking level (*e.g.*, speaking S-2+, S-3) that is closest to the SA's estimated skill level.

A SA applying for the FLAP who already possesses FILR proficiency ratings must identify the following on the Form OI 9731:

- Foreign language;
- Proficiency rating; and
- Date and place of last rating.

The SA must attach a copy of the test results to the Form OI 9731, if available.

The completed Form OI 9731 is filed in the SA's or ASAC's Employee Personnel File (EPF).

420.6 Foreign Language Proficiency Testing.
To be eligible for the program, SAs must demonstrate their foreign language(s) proficiency by attaining a tested FILR foreign language proficiency rating of at least a Speaking Level 2 (S-2). SAs without a current FILR rating will be tested in the foreign language(s) for which they claim proficiency. SAs who have been tested must have a current FILR proficiency rating based on the testing schedule listed in Section 420.6.3. Proficiency testing is required to participate in the FLAP.

An outside testing agency conducts the proficiency testing. The testing agency uses the FILR proficiency testing/rating system as required by Treasury Personnel Manual, Chapter 451.1 and when necessary, is responsible for justifying the validity and reliability of the testing procedures.

All speaking proficiency tests are conducted over the telephone and are taped by the testing agency. No cellular telephones shall be used for testing purposes. The ASAC, Training Team provides the test result to the SAC. The SAC provides the SA with a copy of the test result through his/her ASAC. The test result is used to determine eligibility for participation in the FLAP.

The SAC notifies the Performance and Results Information System (PARIS) Coordinator of the SA's certification. The PARIS Coordinator updates the SA's PARIS employee record to indicate the certification, the foreign language the SA is certified to use, and the expiration date of the certification.

420.6.1 Requesting Proficiency Testing. The SAC must coordinate testing through the ASAC, Training Team. During the first quarter of each year, the SAC of each division must submit a Request, Authorization, Agreement and Certification of Training (SF 182) that identifies all SAs in the division who request to be tested or require retesting. See the retest schedule in Section 420.6.3.

Each SF 182 must contain a roster with the following information for each SA to be tested:

- SA name;
- Social Security Number (SSN);
- Office location;
- Test type - speaking proficiency; and
- Foreign language to be tested.

Submit the completed SF 182 with attached roster and Privacy Act statements to the ASAC, Training Team for submission to, payment of, and scheduling with the testing agency.

The ASAC, Training Team notifies the SAC of the test schedules for their divisions.

420.6.2 Proficiency Ratings. The following are abbreviated descriptions of the speaking skill levels established by the FILR:

> *Speaking 0, No Proficiency (S-0)* – Employee is unable to function in the spoken language. Oral production is limited to occasional isolated words. Has essentially no communicative ability.

Speaking 0+, Memorized Proficiency (S-0+) – Employee is able to satisfy immediate needs using rehearsed utterances. Shows little real autonomy of expression, flexibility or spontaneity. Can ask questions or make statements with reasonable accuracy only with memorized utterances or formulae. Attempts at creating speech are usually unsuccessful.

Speaking 1, Elementary Proficiency (S-1) – Employee is able to satisfy minimum courtesy requirements and maintain very simple face-to-face conversations on familiar topics.

Speaking 1+, Elementary Proficiency, Plus (S-1+) – Employee can initiate and maintain predictable face-to-face conversations and satisfy limited social demands.

Speaking 2, Limited Working Proficiency (S-2) – Employee is able to satisfy routine social demands and limited work requirements. Can handle routine work-related interactions that are limited in scope.

Speaking 2+, Limited Working Proficiency, Plus (S-2+) – Employee is able to satisfy most work requirements with language usage that is often, but not always, acceptable and effective. The individual shows considerable ability to communicate effectively on topics relating to particular interests and special fields of competence.

Speaking 3, General Professional Proficiency (S-3) – Employee is able to speak the language with sufficient structural accuracy and vocabulary to participate effectively in most formal and informal conversations on practical, social and professional topics.

Speaking 3+, Professional Proficiency, Plus (S-3+) – Employee is often able to use the language to satisfy professional needs in a wide range of sophisticated and demanding tasks.

Speaking 4, Advanced Professional Proficiency (S-4) – Employee is able to use the language fluently and accurately on all levels normally pertinent to professional needs.

Speaking 4+, Advanced Professional Proficiency, Plus (S-4+) – Employee's speaking proficiency is regularly superior in all respects, usually equivalent to that of a well-educated, highly articulate native speaker.

Speaking 5, Functionally Native Proficiency (S-5) – Employee's speaking proficiency is functionally equivalent to that of a highly articulate, well-educated

native speaker and reflects the cultural standards of the country where the language is natively spoken.

420.6.3 Testing Schedule. All applicants will be tested as they enter the program and are retested according to their FILR rating:

- Less than S-2 – may be retested on a yearly basis;
- S-2 through S-3+ – must be retested every two years; and
- S-4 and above – must be retested every four years.

420.7 Eligibility Requirements.
A SA who applies to participate in the FLAP must meet the following eligibility requirements to be admitted into the FLAP:

- A permanent full-time or part-time SA.
- A "Successful" rating on their most recent rating of record. The ASAC or SAC must confirm this requirement before a SA is scheduled for testing or, if the SA has a current FILR proficiency rating, before the SA is admitted into the FLAP.
- Attained a tested proficiency rating of at least a Speaking Level 2 (S-2). See proficiency rating definitions in Section 420.6.2.

420.8 Cash Award Amounts.
Pursuant to 5 U.S.C. § 4523, the cash award is based on both proficiency and substantial use of a foreign language in the performance of official duties. The amount of the award may be up to five percent of basic pay for the calendar year. In order to improve proficiency and use, SAs with a higher proficiency rating level and/or greater use in the performance of official duties may be eligible for larger awards. **All awards are subject to the availability of funds.**

420.8.1 Single Foreign Language Awards. Single foreign language award percentages are computed based on the table below. To compute an award percentage, identify the tested FILR speaking skill level and the number of qualifying hours of annual foreign language use. Use the table below to determine the award percentage. For example, a full-time SA with a speaking proficiency rating of S-2+ and 390 hours of foreign language use may be eligible for an award of 2 percent of his/her basic pay.

	Qualifying Hours for Foreign Language Awards and Awards Percentages			
Tested Skill Levels	**Level 1** 209-311 hours used	**Level 2** 312-415 hours used	**Level 3** 416-519 hours used	**Level 4** 520+ hours used
S-3 & above	2% award	3% award	4% award	5% award
S-2 & S-2+	1% award	2% award	3% award	4% award

420.8.2 Multiple Foreign Language Awards. An SA, who has qualifying proficiency ratings and substantial use in more than one foreign language, must submit supporting documentation for each foreign language used. An award percentage is computed for each foreign language. The award percentages for each foreign language are added together to determine the total award percentage, however, the total award may not exceed five percent of the SA's basic pay for the calendar year.

420.8.3 Part-Time Special Agent Awards. A part-time SA who meets the eligibility requirements shall also be considered for a foreign language award. First, the ASAC must determine if the SA's hours of foreign language use for the calendar year meet the part-time substantial use requirement as defined in Section 420.3. If the hours of use do not meet the part-time substantial use requirement, then the SA is not eligible for an award.

If the part-time substantial use requirement is met, the award percentage is computed by determining the appropriate range of qualifying hours in the table in Section 420.8.1 and prorating the hours by the percentage calculated for the part-time substantial use requirement.

For example, an SA who works 16 hours per week and has an S-2 speaking proficiency rating and 110 hours of foreign language use for the calendar year, the award percentage shall be calculated as follows:

- Determine the percentage of the work week for the part-time SA (*e.g.*, 16 hours divided by 40 hours = 40%).
- Prorate the first range of qualifying hours in the table to determine where the 110 hours of foreign language use will fall by multiplying 209 and 311 hours by 40% (209 hours x .40 = 83.6 or 84 hours; 311 hours x .40 = 124.4 or 124 hours). The prorated range becomes 84-124 hours. Since the SA's 110 hours of foreign language use falls within this level, no further calculations are required. If the hours of foreign language use exceed the first level, prorate the second and third levels, as necessary.
- Apply the qualifying prorated hours and the SA's S-2 tested proficiency rating to the table. The SA may be eligible for an award of one percent of basic pay for the calendar year.

420.8.4 Development and Maintenance Costs. Foreign language training, development, and/or maintenance costs will not be deducted from foreign language award amounts.

420.9 Employee Responsibilities.
Since the amount of the award depends on the foreign language proficiency rating and substantial use in the performance of official duties for the calendar year, the number of hours of foreign language use must be verifiable and documented.

An SA who participates in the FLAP must document their foreign language use in their bi-weekly PARIS time reports. The hours of foreign language use must be entered in the "FL" column of the PARIS time report. The foreign language hours are the total number of hours a foreign language was used for specific activities. Foreign language hours are a portion of the Regular and LEAP hours worked each day. SAs must also document the official duties for which the foreign language was used by entering the activities in the "Comments" column of the PARIS time report.

If an SA is tracking use of two or more foreign languages, in addition to documenting the activity in the "Comments" column, he/she must also document the foreign language used and the number of hours the foreign language was used for each activity.

Note: Users should account for hours in the Foreign Language column of the PARIS Time Report only if the agent is in the Foreign Language Award Program.

420.10 Manager Responsibilities.
ASACs and SACs must review and approve authorized foreign language use that is documented in the bi-weekly PARIS time report. Use the foreign language PARIS time report as the supporting documentation for calendar year-end FLAP award recommendations.

Within 30 days following the end of each calendar year, initiate FLAP award recommendations using HR Connect and forward to the SAC or appropriate Deputy Assistant Inspector General for Investigations (DAIGI)/Assistant Inspector General for Investigations (AIGI) for approval. Use the following procedures to submit the FLAP award through HR Connect:

- **Type of Award:** Foreign Language (Law Enforcement)
- **Award Amount**
- **Account Code:** Current fiscal year DIGI accounting code
- **Justification:** "Other" and in the Justification Box, prepare a short justification that includes the following information:

    - Why the award is being recommended;
    - The SA's certification to participate in the FLAP;
    - The number of foreign language hours as documented in approved bi-weekly PARIS time reports; and
    - Any special projects or enhancements to investigations in which the foreign language was used.

- **Comments:** Enter any additional information the Bureau of the Fiscal Service (BFS) should be aware of in processing the award.
- Sign the award recommendation as Initiating Official.

- Attach the applicable PARIS time reports.

The SAC retains a copy of each award recommendation.

420.11 Approving Official Responsibilities.
The SAC is the approving official for award recommendations submitted for an SA. The appropriate AIGI is the approving official for award recommendations submitted for an ASAC. The SAC must certify the availability of award funds with the Operations Division. After review, approval, and certification of funds, the SAC, DAIGI, or AIGI submits the award through HR Connect for processing by the BFS. The SAC forwards a copy of the approved award package to the respective ASAC for retention in the SA's EPF or for ASACs, retains a copy in the ASAC's EPF. The ASAC is responsible for ensuring the SA receives a copy of the award package.

430.12 Reconsideration Procedures.
Since an outside testing agency administers the foreign language proficiency test, test results may not be grieved. If the SA disagrees with the test result and the SAC cannot immediately resolve the disagreement, the SA can request that the testing agency conduct a formal review of the test result in dispute. The testing agency will issue a second opinion on the test results. If the SA still disagrees with the test results, the SA will be scheduled for retesting on the foreign language for which the test result is in dispute. The testing agency must conduct the retest. The retest rating is the SA's official rating and cannot be disputed. The SA may be retested according to the testing schedule in Section 420.6.3.

An SA, who disagrees with the number of hours certified by the ASAC and SAC, or the hours approved by the AIGI, may submit requests for reconsideration. The SA must state the disagreement in writing and submit it to his/her ASAC within 15 days of the SA becoming aware of the decision with which he/she disagrees. The SA must state the reasons and facts for his/her disagreement and must attach any available evidence or documents that support his/her request.

Once foreign language use and/or testing issues have been resolved, the amount of the cash award will be determined by using the computations contained in Section 420.8. Any errors in mathematics or in applying the computation table must be immediately rectified.

420.13 Program Timetable.

January:	ASAC must initiate award recommendations for SAs for the previous calendar year to the SAC. The SAC must initiate award recommendations for ASACs.
January – February:	SAC or appropriate DAIGI/AIGI reviews and approves award recommendations. After funds have been certified and

	awards approved, the SAC forwards awards recommendations to BFS for processing. A copy of the award package is sent to the SA's ASAC for retention in the SA's EPF. A copy of an ASAC's award package is retained by the SAC in the ASAC's EPF.
January – March:	New applicants are tested or current participants are retested as required by the proficiency rating levels and retesting schedule.
January - December:	SAs and ASACs approved to participate in the FLAP, track their hours and activities in their PARIS time reports for the current calendar year. The ASAC or SAC approves foreign language hours documented in bi-weekly PARIS time reports.
October - December:	SAs may apply for participation in the FLAP by submitting a completed Form OI 9731 to their SAC through their ASAC. ASACs may apply for participation in the FLAP by submitting a completed Form OI 9731 to their SAC. SACs submit SF 182s to the ASAC, Training Team identifying SAs who require testing or retesting.

DATE: January 1, 2020

CHAPTER 400 – INVESTIGATIONS

(400)-430 False Personation Investigations

430.1 Overview.
False personation investigations involve external attempts to corrupt tax administration by individuals or entities that misidentify themselves or who they represent for the purpose of perpetuating their deception scheme. This section includes the following information related to false personation investigations:

- Authority
- False Personation Investigations
- Misuse of Treasury Name or Symbol Investigations

430.1.1 Acronyms Table.

430.2 Authority. The authority of the Treasury Inspector General for Tax Administration (TIGTA) to investigate false personation cases is derived from the Inspector General (IG) Act, Treasury Order (T.O.) 115-01, and the Internal Revenue Service Restructuring and Reform Act of 1998 (RRA 98).

430.3 False Personation Investigations.
TIGTA investigates allegations regarding impersonations of Internal Revenue Service (IRS) employees. The purpose of these investigations is to protect the integrity of the IRS by detecting and seeking prosecution of persons who impersonate IRS employees. Title 18, U.S.C. § 912, *Officer or employee of the United States*, applies to whoever falsely assumes or pretends to be an officer or employee acting under the authority of the United States or any department, agency or officer thereof, and acts as such, or in such pretended character demands or obtains any money, paper, document, or thing of value.

In circumstances in which a person or persons are using words, titles, abbreviations, initials, symbols, or emblems which could reasonably be interpreted or construed as conveying the false impression that such advertisement, solicitation, business activity, or product is in any manner approved, endorsed, sponsored, or authorized by, or associated with, the Department of the Treasury, TIGTA has authority to investigate under Title 31 U.S.C § 333, *Prohibition of misuse of Department of the Treasury names, symbols, etc.* See Section 430.4, *Misuse of Treasury Name or Symbol Investigations.*

Upon receipt of an impersonation allegation, Special Agents (SAs) must obtain, at a minimum, the following information from the complainant in an alleged impersonation of an IRS employee:

- Name, address, and telephone number of the complainant;

- Whether the complainant or any of the complainant's family members have any tax matters pending before the IRS or State and local tax authorities;
- A physical description of the alleged impersonator, if available;
- A description of any documents, credentials or badges that may have been exhibited;
- A detailed narrative description of the entire incident from the complainant; and
- Whether the alleged impersonator intends to return.

In addition to obtaining the above information from the complainant, immediately query IRS records to determine:

- If the alleged impersonator is in fact an IRS employee;
- If the alleged impersonator is in fact an IRS employee using a pseudonym;
- If the alleged impersonator is using an IRS employee's name; and
- If the contacted taxpayer has open activity with any IRS component.

To determine whether an alleged impersonator is an IRS employee using a pseudonym, contact the IRS's Office of Privacy, Governmental Liaison and Disclosure, Incident Management and Employee Protection Office, via e-mail to pseudonym@irs.gov.

SAs should contact State authorities to ensure that the alleged impersonator is not a legitimate State official, as necessary.

When processing an intake in the Criminal Results Management System (CRIMES), use violation code 550 – IMPERSONATION.

430.4 Misuse of Treasury Name or Symbol Investigations.

Pursuant to T.O. 115-01, TIGTA has the authority to investigate possible violations of, and to assess civil penalties and issue cease and desist letters under, 31 U.S.C. § 333, Misuse of Treasury Name or Symbol, involving:

- The misuse of the name or symbol of the IRS, the IRS Office of Chief Counsel, the IRS Oversight Board, or the title or name of the IRS Commissioner, of any IRS employee, or of any employee of the IRS Office of Chief Counsel or of the IRS Oversight Board;
- The misuse of the name or symbol of TIGTA, or the title or name of the TIGTA or of any TIGTA employee; or
- The misuse of the name or symbol of the Department of the Treasury, or the title or name of the Secretary or of any Treasury employee, in connection with activities within the jurisdiction of TIGTA.

For activity to constitute a violation of this statute, it must satisfy the following criteria:

- The activity must include the use of one of the names, titles, symbols, or emblems described in subsection (a)(1) through (a)(6) of 31 U.S.C. § 333;
- The name, title, symbol, or emblem must be used “in connection with, or as a part of, an advertisement, solicitation, business activity, or product;” and
- The use of the bureau name, title, symbol, or emblem must be "in a manner that could reasonably be interpreted or construed as conveying the false impression that such advertisement, solicitation, business activity, or product is in any manner approved, endorsed, sponsored, or authorized by, or associated with" the bureau or its officers or employees.

Contact the Operations Division via e-mail to *TIGTA Inv Operations for assistance with applying these criteria.

Upon receipt of an allegation related to the misuse of Treasury/IRS names or seals, immediately query Government sources of information to determine if the alleged subject is affiliated with the Department of the Treasury. When it is determined that the alleged subject or entity is not affiliated with the Department of the Treasury, initiate a misuse of Treasury name or symbol Investigation.

When processing an intake in CRIMES, use violation code 506 – MISUSE OF TREASURY/IRS NAMES OR SEALS.

430.4.1 Cease and Desist Letters. Once it has been determined that a violation of 31 U.S.C. § 333 has occurred, a cease and desist letter may be issued to an individual (or entity) advising that the activity is in violation of 31 U.S.C. § 333 and instructing the individual (or entity) to immediately cease the activity that violates the statute. The cease and desist letter requires the individual (or entity) to respond to TIGTA within 10 business days. If the individual (or entity) persists in violating 31 U.S.C. § 333, TIGTA may seek civil or criminal action. Prior to requesting the issuance of a cease and desist letter, the assigned SA will inform the U.S. Attorney’s Office of the activity and of TIGTA’s intention to issue a cease and desist letter, and obtain their concurrence.

430.4.1.1 Requests for Cease and Desist Letters. Requests will originate with the assigned SA. The Assistant Special Agent in Charge (ASAC) and/or the Special Agent in Charge (SAC), and the Operations Division should be consulted as necessary, prior to forwarding the request in order to ensure that all relevant information is included.

430.4.1.2 Information in Request. The request should reflect the need for using a cease and desist letter, and include the following:

- Case name and number;
- The name and address of the individual, corporation, partnership, agency, institution, or other recipient of the cease and desist letter;

- A statement of the activity that violates 31 U.S.C. § 333, including any visual examples of the violating activity;
- The U.S. Attorney's Office (*i.e.*, Federal district) that TIGTA has coordinated with; and
- The name and telephone number of the SA conducting the inquiry.

The request package will include a completed cease and desist letter template and supporting information related to the alleged offense (*e.g.*, scanned copy of improper letterhead or Report of Investigation (TIGTA Form OI 2028R).

430.4.1.3 Submission of Requests and Decision to Issue. All requests to issue a cease and desist letter will be approved by the ASAC and the SAC before they are forwarded to the Operations Division.

The SAC will forward the request to the Operations Division via e-mail to *TIGTA Inv Operations. The Operations Division will conduct an initial review of the request and forward it to TIGTA Counsel. TIGTA Counsel will review the request and the completed template for legal sufficiency. After review, Counsel will return the request to the Operations Division, who will forward the electronic document to the appropriate Assistant Inspector General for Investigations (AIGI) for signature. Once the letter has been approved by the appropriate AIGI, the Operations Division will send an electronic copy of the approved letter to the requesting SA, ASAC, SAC, and the *TIGTA Inv Operations inbox. The electronically signed letter is the final document and may be served as deemed appropriate.

To properly capture this information in CRIMES, create a "Civil Referral." Select "Other Civil" then click "Save." When the "TIGTA CEASE AND DESIST ORDER" is issued, add a "TIGTA CEASE AND DESIST ORDER" Referral Outcome with the issuance date. In most instances, select Criminal Status code 3, "AUSA - DECLINED IN LIEU OF CIVIL PROCEEDINGS," on the Criminal Referral, if appropriate.

430.4.2 Assessment of Civil Penalties. (Reserved)

DATE: July 1, 2021

CHAPTER 400 – INVESTIGATIONS

(400)-440 Fraud and Schemes Division

440.1 Overview.
The Treasury Inspector General for Tax Administration (TIGTA), Office of Investigation (OI), Fraud and Schemes Division (FSD) is comprised of the following three groups:

- Investigation Development Group;
- Fraud Development Group; and
- Complaint Management Team.

This section includes information related to the following:

440.1.1 Acronyms Table

440.2 FSD Role.
FSD supports the OI mission by:

- Developing proactive leads and investigations related to administrative and criminal violations within TIGTA's jurisdiction;
- Providing analytical support of IRS Records, Bureau of the Fiscal Service (BFS) records and other records to enhance field investigations;
- Processing information sent to the TIGTA hotline; and
- Assisting with various records request and records management.

440.3 Investigation Development Group.
The Investigation Development Group (IDG) primarily focuses on the following activities in furtherance of the mission of FSD and OI:

- ***, develops proactive leads and investigations to detect administrative and/or criminal violations associated with misuse of IRS systems by internal and external users and misuse of IRS records by IRS employees ***;
- Through *** develops proactive leads and investigations to detect criminal violations associated with IRS related U.S. Treasury checks;
- ***, obtains information and/or provides analytical support of IRS records and BFS records to enhance investigations in other divisions;

- ***, provides analytical support of IRS related U.S. Treasury checks to enhance investigations in other divisions;
- Provides testimony/evidentiary guidance and advice during criminal and administrative proceedings; and
- The point of contact for changes, problems, enhancements of the IRS Security Audit and Analysis System, ***

440.4 Fraud Development Group.
The Fraud Development Group (FDG) primarily focuses on the following activities in furtherance of the mission of FSD and OI:

- Through the use of ***, develops proactive leads and investigations to detect criminal violations related to IRS impersonation schemes and misuse of U.S. Treasury symbols and/or names ***;
- Through ***, develops proactive leads and investigations to detect criminal violations related to domestic and international attempts to obstruct Federal tax administration;
- Through ***, develops proactive leads and investigations to detect administrative and/or criminal violations related to IRS employee related fraud and integrity, which do not involve IRS or Bureau of Fiscal Services records (e.g. Unauthorized Access, U.S. Treasury Checks);
- Develop leads and investigations related to *** delegated as priority by the OI executive team;
- ***, provide analytical support of IRS and BFS records to enhance investigations in other divisions;
- *** ; and
- Provide testimony/evidentiary guidance and advice during criminal and administrative proceedings.

440.5 Managing Leads and Requests for Assistance.
***
Reporting of potential misconduct or fraud violations will be ***.

FSD initiates leads from ***. FSD may, also, develop complex leads, multi-jurisdictional leads, international leads, or proof of concept leads that result in an investigation being generated within FSD. FSD will document investigative activities in the *** .

If not warranted for investigation, FSD will close the lead to file and document the reasons ***.

OI employees will submit a *** to FSD *** for analytical support of a complaint or investigation. ***. FSD will attempt to complete all ***. If completion of the ***, update the description box for the *** to include an estimated completion date. FSD will complete the analysis and report the results in ***. ***

FSD will create a research folder *** associated complaint or investigation. Upon completion, the *** will be approved by appropriate FSD manager prior to being returned to the OI employee who submitted the ***.

440.5.1 Referring Misconduct or Fraud Violations to the Special Investigations Unit
FSD will transfer to the Special Investigations Unit (SIU) all allegations of misconduct involving TIGTA employees, with the exception of alleged impropriety or misconduct by a SIU employee or TIGTA senior executives.

440. 6 Complaint Management Team.
The Complaint Management Team primarily focuses on processing information the hotline receives, and assisting with record requests and the records management process. ***

CHAPTER 400 – INVESTIGATIONS

(400)-450 Body Worn Camera Program

450.1 Overview.
This section outlines the policies and procedures governing the Office of Investigations (OI) body worn camera (BWC) program. This policy does not govern the use of surreptitious recording devices in undercover operations.

This section includes information related to the following:

450.1.1 Acronyms Table.

450.2 Body Worn Cameras.
BWCs provide an additional layer of safety for the special agent (SA) and can improve public trust, transparency, and accountability. BWCs allow for accurate documentation of contacts between SAs, IRS employees, and the public, which can help resolve complaints made against an SA.

BWC recordings can be used as evidence for investigative and prosecutorial purposes in the event an SA is threatened or assaulted during a contact or if there is a use of force or critical incident. It should be noted that recordings may depict things that the SA did not see or hear, and/or the SA may have heard or seen things that were not recorded by the BWC. While the recording depicts visual information from the scene,

the human eye and brain are highly likely to perceive some things in stressful situations differently than how the camera records them.

450.3 Body Worn Camera Program.
The Assistant Special Agent in Charge (ASAC), Technical Operations Group provides oversight of the BWC program under the direction of the Special Agent in Charge (SAC), Technical and Firearms Support Division (TFSD). The BWC Program Manager is responsible for the daily management of the program. The BWC Program Manager will periodically review BWC recordings to ensure that the equipment is operating properly and that SAs are using the devices appropriately and in accordance with OI's policy.

450.4 Joint Operations.
When conducting enforcement operations with another law enforcement agency, TIGTA SAs will comply with OI's BWC policy.

The TIGTA team leader for the enforcement operation shall discuss the use of BWCs with the other agency's team leader prior to the enforcement operation. The case agent will document these discussions on TIGTA Form OI 6501, *Chronological Case Worksheet*.

The SAC shall notify the appropriate Assistant Inspector General for Investigations (AIGI) or Deputy Assistant Inspector General for Investigations (DAIGI) if there is an unresolved conflict with the other law enforcement agency regarding TIGTA's intent to deploy BWCs during an enforcement operation when TIGTA is the lead agency.

450.5 When to Use Body Worn Cameras.
SAs shall activate BWCs when such use is appropriate for the proper performance of their official duties and where recording is consistent with OI policy and the law.

450.5.1 Deployment for Enforcement Operations. BWCs will be deployed for TIGTA enforcement operations. All SAs participating in the enforcement operation will be equipped with BWCs. SAs will activate their BWCs to record contacts with individuals during enforcement operations.

For the purposes of this section, enforcement operations include arrests, search warrants, and armed escorts. See Section 450.9 for additional information.
The TIGTA team leader should inform the BWC Program Manager if a member of the Undercover Cadre participated in the enforcement operation, and the BWC Program Manager will document this in the BWC log.

450.5.2 Deployment for Threat Interviews. Due to their exigent nature, threat interviews are not always planned and may be conducted extemporaneously.

Therefore, there may be instances when it is not possible to deploy BWCs for threat interviews. However, every effort should be made to utilize the BWC when possible.
450.5.3 Deployment in Other Instances. SAs may request approval from the ASAC to deploy BWCs in other instances (*e.g.*, interview of a subject or third party witness who has an extensive criminal history or history of violence, surveillance, etc.) where it may be prudent to record the interactions. See Section 210.20.1.2 for recording custodial interviews.

450.6 Placement of Body Worn Camera.
The BWC should be worn on the outside of the ballistic vest or outermost garment to ensure the best field of view. SAs should ensure the BWC is not obstructed by clothing, lanyards, accessories, etc.

450.7 Activation of Body Worn Cameras.
SAs will activate their BWC at the direction of the TIGTA team leader of the enforcement operation. The team leader will determine when to activate the BWCs and will ensure that each member of the enforcement team has activated the BWC prior to beginning the enforcement action. The SA will verbally state, "*Body camera activated*" and his/her name, the date and time.

SAs shall record the activities until they are concluded or, if executing a search warrant, until the location to be searched is secured and all subjects have been searched. See Section 450.7. To ensure the integrity of the recording, the BWC must remain activated until the activity is completed unless the contact moves into an area restricted by this policy. See Section 450.13.

450.8 Deactivation of Body Worn Cameras.
SAs will deactivate their BWCs at the direction of the TIGTA team leader for the enforcement operation. Prior to deactivating the BWC, the SA will verbally state the date, time, and reason for the BWC's deactivation.

When executing a search warrant, the team leader can authorize the team to deactivate the BWC once the location to be searched has been secured and all subjects have been searched. The TIGTA team leader will use his or her discretion to determine whether team members participating as outside cover during the execution of the warrant should continue to record.

BWCs have a limited battery life. If the enforcement operation is of such a duration that the BWC should be deactivated to conserve power and/or storage, the TIGTA team leader can authorize deactivation.
The TIGTA team leader will collect all BWCs from the team members and return the BWCs to the BWC Program Manager. See Section 450.11.

An SA may deactivate the BWC to obtain medical attention.

450.9 Recording During the Enforcement Operation.
Whenever possible, SAs should inform individuals at the beginning of the contact that they are being recorded (*e.g.*, "Sir/Ma'am, I am advising you that our interaction is being recorded.") If the BWC must be deactivated during an operation, the SA should verbally state that the BWC is being deactivated and state the date, time, and reason for the deactivation.

In locations where individuals have a reasonable expectation of privacy such as a residence, and only during non-enforcement activities, individuals may decline to be recorded unless the recording is being made pursuant to an arrest or search of the residence or individuals. See Section 450.13.

450.10 Documenting Use of Body Worn Cameras.
Upon the conclusion of the enforcement operation or activity (*e.g.*, threat interview, surveillance, *etc.*), the case agent will document in TIGTA Form OI 6501, *Chronological Case Worksheet*, that a recording was made and provide a brief summary of the activity.

The summary should include the following information and may be part of the overall memorandum documenting the law enforcement activity:

- The names of the team members participating in the activity or operation;
- Whether or not all SAs were wearing BWCs during the activity or operation;
- Whether or not all BWCs were activated prior to the activity or operation;
- If any BWCs malfunctioned or were inoperable during the activity or operation;
- If any BWCs were not activated prior to, or during, the activity or operation;
- If any BWCs were turned off during the activity or operation; and
- If any BWC recording was interrupted or terminated during the activity or operation.

450.10.1 Failure to Activate Body Worn Camera. If an SA fails to activate the BWC, fails to record the entire contact, or interrupts the recording, the SA shall document in a memorandum through the SAC to the appropriate AIGI or DAIGI and the BWC Program Manager the following:

- Why the recording was not made;
- Why the recording was interrupted; and/or
- Why the recording was terminated.

An intentional failure to activate the BWC or the unauthorized termination of a BWC recording may result in disciplinary action.

450.11 Download and Storage of Body Worn Camera Recordings.
Upon conclusion of the enforcement operation or activity, the TIGTA team leader will collect all BWCs and return them to the BWC Program Manager or DTA using express shipping. The team leader will complete TIGTA Form OI 4500, Body Worn Camera Worksheet, and include it with the BWCs when returning. The BWC Program Manager will download all BWC recordings. Each file shall contain the date and time of the recording, BWC identifier, and assigned SA. An audit log is automatically created and maintained on the history of every recording.

If a physical altercation or other significant incident occurs during the enforcement operation, the BWCs will be delivered to the BWC Program Manager or DTA on site to download the BWC recordings.

If the BWC recording is deemed evidence, the BWC Program Manager or DTA will create an evidence disc containing the recording from the enforcement operation and provide it to the case agent for entry into evidence. The BWC Program Manager or DTA will complete a TIGTA Form OI 5397, *Evidence Custody Document*, documenting the chain of custody from the BWC Program Manager or DTA to the case agent.

If needed, a working copy of the BWC recording may be provided to the case agent.

450.12 Records Retention.
BWC recordings will be securely stored on a dedicated server. All recordings are agency records and should be disposed of according to TIGTA's records retention policy.

For BWC recordings deemed as evidence, the SA will adhere to the OI evidence policy. See Section 190.

450.13 Restrictions on Use.
SAs equipped with BWCs should be mindful of locations where recording may be considered insensitive, inappropriate, or prohibited by privacy policies. BWCs shall only be used in conjunction with official law enforcement duties and not personal activities.

BWCs shall not be used to record:

- Undercover operations;
- Communications with other SAs without the written permission of an AIGI or DAIGI; and
- Locations where individuals have a reasonable expectation of privacy such as a restroom or locker room without the permission of an AIGI or DAIGI.

450.14 Body Worn Camera Equipment.
SAs shall only use BWCs issued by OI. SAs should exercise reasonable care when using BWCs to ensure their proper functioning. SAs should ensure that the BWC is fully charged before its deployment.

SAs will notify the BWC Program Manager of any equipment malfunctions as soon as possible.

450.14.1 Loss or Theft of Equipment. All SAs will report the loss or theft of a BWC to their immediate supervisor as soon as practical but within 24 hours of the discovery of the loss or theft. The immediate supervisor shall notify the Special Investigations Unit and the SAC-TFSD.

450.15 Body Worn Camera Recordings.
The BWC equipment and all data, images, video, and metadata captured, recorded, or otherwise produced by the equipment is the sole property of TIGTA. SAs shall not edit, alter, erase, duplicate, copy, share, or otherwise release, disclose or distribute in any manner, any BWC recording, without prior written authorization from the respective AIGI or DAIGI.

SAs must obtain written approval from the TIGTA Disclosure Branch prior to any disclosure of information (*i.e.*, audio or video recording, etc.) recorded by the BWC. See Chapter 700, Section 70. All requests for disclosure of information should be coordinated through the BWC Program Manager.

Unauthorized accessing, copying, or releasing files is strictly prohibited.

450.15.1 Deleting Recordings. Any request to delete a portion or portions of the recordings (*e.g.*, accidental recording) must be submitted in writing and approved by the respective AIGI or DAIGI. The request must be made in a memorandum and must state the reason(s) for deleting the recording. The approved memorandum will be provided to the ASAC-Technical Operations Group, TFSD. The recording will only be deleted after the approved memorandum is received by the ASAC.

All requests and final decisions will be maintained by the BWC Program Manager. See Section 450.15.

450.15.2 Access and Review of Body Worn Camera Recordings. All accesses will be audited to ensure that only authorized users are accessing the data for legitimate and authorized purposes.

Any requests to review body worn camera recordings must be made in a memorandum to the BWC Program Manager. The memorandum must state the reason(s) for the request to review the recording.

450.15.3 Permitted Reviews of Body Worn Camera Recordings. An SA shall be entitled to access the audio and video data derived from the BWC equipment issued to him/her to defend against allegations of misconduct or poor performance during the recorded enforcement activity. SAs will not share audio and video data files without an official purpose. Audio and video data files will be not provided where a use of force or critical incident occurs.

SAs who are the subject of an investigation may review their own BWC recording prior to providing any statements to, or being interviewed by, SIU. The SA may review the recording with his/her attorney or other representative.

Following a use of force or critical incident, the involved SA shall be given the opportunity to view his or her own BWC recording prior to giving a formal statement. SAs who are witnesses to a use of force or critical incident shall also be allowed to view their own BWC recording prior to giving a formal statement.

SIU may review BWC recordings in connection with an official SIU investigation.

BWC recordings may be used to provide information for training purposes with the permission of all TIGTA SAs captured by the audio or video.

450.15.4 Prohibited Reviews of Body Worn Camera Recordings. Supervisors may not review BWC recordings solely for evaluating the SA's performance during the operation or for conducting performance appraisals.

450.16 Freedom of Information Act Requests.
Recordings from BWCs may be subject to release pursuant to the Freedom of Information Act (FOIA). Any request for records made pursuant to FOIA received by a TIGTA employee should be forwarded to TIGTA's Office of Chief Counsel's Disclosure Branch, which is responsible for processing and responding to the request. See Chapter 700, Section 60.

Any requests for the release of BWC recordings will be forwarded to the BWC Program Manager. The BWC Program Manager will, at a minimum, review all BWC footage that is proposed for release and specify which parts of the footage may be released and which parts need to be redacted, along with the relevant justifications, and provide a complete copy of the BWC recording to the Disclosure Branch with the suggested redactions and justifications in writing. The Disclosure Branch will review the suggested redactions and justifications and provide its comments and/or concurrence to the BWC Program Manager. Upon receiving concurrence from the Disclosure Branch, the BWC Program Manager will use the appropriate redaction software to redact the BWC recording. The BWC Program Manager will return the redacted BWC recording to the Disclosure Branch for FOIA response.

450.16.1 Exclusions. The U.S. Congress has provided special protection in the FOIA for three narrow categories of law enforcement and national security records. The provisions protecting those records are known as “exclusions.” The first exclusion protects the existence of an ongoing criminal law enforcement investigation when the subject of the investigation is unaware that it is pending and disclosure could reasonably be expected to interfere with enforcement proceedings.

The second exclusion is limited to criminal law enforcement agencies and protects the existence of informant records when the informant’s status has not been officially confirmed.

The third exclusion is limited to the Federal Bureau of Investigation and protects the existence of foreign intelligence or counterintelligence, or international terrorism records when the existence of such records is classified.

Records falling within a FOIA exclusion are not subject to the requirements of the FOIA.

450.16.2 Exemptions. The U.S. Congress established certain categories of information that are not required to be released in response to a FOIA request because release would be harmful to a government or private interest. These categories are called "exemptions" from disclosures. However, even if an exemption applies, agencies may use their discretion to release information when there is no foreseeable harm in doing so and disclosure is not otherwise prohibited by law.

There are nine categories of exempt information. Exemption 7 of FOIA, often referred to as the law enforcement exemption, is the most common exemption used by law enforcement.

See Chapter 700, Section 60. Information about FOIA can be found at https://www.foia.gov/faq.html.

450.17 Privacy Act Referrals.
The Privacy Act of 1974, 5 U.S.C. § 552a (Privacy Act or Act), provides safeguards for individuals against an invasion of personal privacy through the misuse of records by Federal agencies. The Act balances the individual’s personal privacy interest against the Government’s need to maintain information about individuals.

TIGTA is authorized under the provisions of the Privacy Act to refer documents and results of investigations to other law enforcement agencies. Specifically, under the system of records under which TIGTA is currently operating, TIGTA may disclose pertinent information to appropriate Federal, State, local or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the

disclosing agency (*i.e.*, TIGTA), becomes aware of a potential violation of civil or criminal law or regulation, etc.

Privacy Act referrals of TIGTA records, including BWC recordings, to another law enforcement agency must be reviewed by TIGTA's Office of Chief Counsel with the exception of the following:

- Referrals to the Department of Justice;
- Referrals to the Internal Revenue Service (IRS); and
- Referrals of information concerning a threat of imminent danger, or death, or physical injury.

SAs will follow the procedures for Privacy Act referrals as detailed in Chapter 700, Section 70. After TIGTA's Office of Chief Counsel determines there is legal authority to refer body camera recordings to another law enforcement agency, the Privacy Act referral will be forwarded to the BWC Program Manager to download the BWC recording to a compact disc. The BWC Program Manager will, at a minimum, review all video footage that is proposed for release and specify which parts of the video that may be released and which parts that need to be redacted, along with the relevant justifications in writing. The BWC Program Manager will use the appropriate redaction software to redact the video.

450.18 Supervisory Responsibilities.
Supervisory personnel shall ensure that all SAs receive the required training on the use of BWCs in accordance with OI policy and procedures.

450.19 Training.
All SAs must complete a TFSD-approved and/or TFSD-provided training program to ensure the proper use and operation of the BWC and compliance with privacy and civil liberties laws. Additional training will be provided at periodic intervals to ensure the SA's continued proficiency in the use of BWCs.

For training purposes, BWCs will be used during the Special Agent Basic Training Program and the Special Agent Advanced Training Program.

To ensure operational readiness and proficiency in the use of BWCs, the BWC Program Manager and DTAs, under the BWC Program Manager's direction, will keep abreast of significant changes in technological capabilities by attending training and maintaining liaison and/or working with other Federal law enforcement agencies that use the technology on a regular basis. The BWC Program Manager and DTAs will also receive periodic training on privacy and civil liberties laws.

DATE: October 1, 2021

CHAPTER 400 – INVESTIGATIONS

(400)-460 Tax Refund Check Investigations

460.1 Overview.
This section establishes Office of Investigations (OI) policy and procedures regarding the investigation of alleged stolen tax refund checks, issued by the U.S. Department of the Treasury.

460.1.1 Acronyms Table.

460.2 Authority.
OI's authority to investigate tax refund check fraud is established by the Inspector General Act of 1978, as amended, and is further described in Treasury Order 115-01.

OI will only initiate leads (*i.e.*, proactive analysis of potentially fraudulent activity to develop evidence of a crime) or investigations if the alleged check or electronic payment fraud involves tax refund checks, Internal Revenue Service (IRS) check numbers, or checks that pertain to Federal tax administration. TIGTA special agents (SAs) shall not investigate matters that do not involve the programs and operations of the IRS. This type of investigation must have a clear nexus to Federal tax administration. Misuse of the Treasury seal on a check alone is not sufficient to justify initiating an investigation unless it involves a tax refund check.

460.3 Check Fraud Intakes.
Check fraud information is vast and changes frequently. Therefore, OI has directed the Fraud and Schemes Division (FSD) to appoint a tax refund check national coordinator (Coordinator) to serve as a conduit for information and training in matters associated to check fraud. FSD has also expanded their SharePoint site to include training material and information concerning check fraud. Contact the Coordinator with questions.

Due to the volume associated with IRS refund check fraud, SAs are not required to enter every allegation of IRS refund check fraud into the Criminal Results Management

System (CRIMES), except when the complaint is received from an IRS employee or the impacted taxpayer.

Before entering an intake into CRIMES, the SA must review the XXXXXX XXXXXXXXXX XXXXXXX XXXXXXXXXXX to confirm that the check has not been included as part of an existing lead, complaint, or investigation.

460.4 Criteria to Open a Lead or Investigation.
OI will only initiate investigations involving IRS programs and operations as described under Section 460.2. Often times the agency directing the Bureau of the Fiscal Service (BFS) to issue a Treasury check is annotated on the face of the Treasury check. In circumstances where the issuing agency is unclear, contact the tax refund check national coordinator (Coordinator) for guidance. Initiate a Request Assistance Form (RAF) in CRIMES for FSD assistance.

460.4.1 Identifying a U.S. Tax Refund Check. To be considered a U.S. tax refund check, whether authentic, altered, counterfeit, or forged, it must include the XXXX XXXXXXXX XXXXXXX XXXXXX, XXXXXXXXX, and one of the following:

- XXX XXXXX XXXXXXXX XXXX XXXXX XX XXXXXXXX;
- XXX XXXXX XXXXXX;
- XXX XXXXXXX XX XXX XXXX XXXX.
-

See the XXX XXXXXX XXXXX XXXXXXXXXXXXXX XXXXXXXXXX for more information on identifying a U.S. tax refund check or contact the Coordinator.

460.5 Tax Refund Check National Coordinator.
The Coordinator is a SA assigned to FSD. The Coordinator's primary responsibilities include the following:

- Function as OI's tax refund fraud subject matter expert;
- Perform liaison activities with BFS and the Treasury Office of Inspector General (Treasury OIG);
- Coordinate all OI requests for BFS assistance;
- Develop and deliver training and briefings for both internal and external audiences;
- Identify check fraud activity for potential proactive lead development based on investigative potential and agency resources;
- Coordinate the assignment of tax refund check RAFs and leads;
- Monitor the inventory of tax refund check RAFs and leads; and
  Ensure that RAFs for tax refund check fraud analysis are completed in a timely manner.

460.6 Requests from Law Enforcement Agencies.
TIGTA will not be a conduit for other law enforcement agencies (LEA) to gain access to U.S. Treasury check information. TIGTA's access to and disclosure of return information, which by definition, includes some of the information on the front of a tax refund check, is governed by 26 U.S.C. § 6103. Investigative disclosures of information are discussed in Chapter (400)-70; the disclosure rules for return information as codified in 26 U.S.C § 6103 are discussed in Chapter (700)-50; and the procedures to release a Report of Investigation (ROI) to another agency are discussed in Chapter (700)-70.

Requests for non-tax refund check data will be referred to the BFS via paymentintegrity@fiscal.treasury.gov.

460.7 Evidence.
Tax refund and counterfeit tax refund checks obtained during the course of an investigation are evidence and should be handled in accordance with Section 190 of this chapter.

460.7.1 Checks Held as Evidence. If an SA secures U.S. Treasury checks as evidence, the SA should send the Coordinator a listing of these checks. The Coordinator will inform BFS that the checks will be held as evidence.

460.7.2 Disposal of Evidence. Treasury checks should be returned to BFS with a Form 3210, *Document Transmittal*, to:

> Bureau of the Fiscal Service
> Philadelphia Financial Center
> Attention: Custodian of Records
> 13000 Townsend Road
> Philadelphia, PA 19154
> Tel. 855-868-0151

Before returning the checks to BFS, contact the Coordinator who will notify BFS to expect the package.

460.8 Calculating Loss.
The United States Sentencing Commission Guidelines Manual, § 2B1.1 states that "intended loss means the pecuniary harm that the defendant purposefully sought to inflict," and, "actual loss means the reasonably foreseeable pecuniary harm that resulted from the offense."

For sentencing purposes under § 2B1.1, the "General Rule" states that the "loss is the greater of the actual loss or the intended loss." The actual financial loss from check fraud is the amount of cash actually obtained by the subject. For example, if a subject deposits an altered $5,000.00 tax refund check, and the bank allows him or her to

withdraw $3,000.00 cash before freezing the funds, the intended loss is $5,000.00, and the actual loss is $3,000.00.

460.9 Restitution and Identifying Victims.
Restitution calculations rely on the actual financial loss to any combination of five potential victims: the financial institution, the money services business (MSB), the Check Forgery Insurance Fund (CFIF), the IRS (or the issuing agency), and/or the taxpayer. The Coordinator should be consulted to assist in establishing restitution amounts.

The address for restitution payments to BFS (for the CFIF) is:

Bureau of the Fiscal Service
Attention: Accounting
13000 Townsend Road
Philadelphia, PA 19154
Tel. 855-868-0151

The address for restitution payments to the IRS is contained in Section 280, *Employee Investigations*.

460.10 Spurious Checks.
OI may obtain spurious tax refund checks. These checks can be printed by BFS with whatever name, address, and dollar amount deemed necessary for an investigation. BFS processes spurious checks with rubber gloves and will deliver these checks (with unsealed envelopes) to the case agent. OI must follow the procedures for obtaining spurious checks. See Chapter (600)-50.9.

Because spurious checks have been funded by TIGTA and printed by BFS, they are authentic checks with monetary value. The checks can be negotiated at a bank or MSB.

460.10.1 The U.S. Postal Inspection Service and Office of Inspector General. SAs will consult with the U.S. Postal Inspection Service and/or U.S. Postal Service Office of the Inspector General in cases involving the alleged theft of U.S. Treasury checks from the mail. A discussion of disclosures in connection with joint investigations involving return information is included in Chapter (400)-70.7.1.

DATE: July 1, 2020

CHAPTER 400 – INVESTIGATIONS

(400)-470 Psychophysiological Detection of Deception Program

470.1 Overview.
This Section outlines the policies and procedures governing the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations (OI) Psychophysiological Detection of Deception (PDD), or "Polygraph," Program as an investigative tool. The polygraph examination is a forensic instrument that is used to measure psychophysiological changes. It is an investigative tool used by a certified polygraph/PPD examiner to detect deception. Polygraph examinations are interviews; interviewees must be provided the appropriate forms and notices. See Section 210.
This Section contains the following:

- Polygraph Program
- Qualification and Selection of Polygraph Examiners
- Training and Certification of Polygraph Examiners
- When to Request a Polygraph Examination
- Authorization and Approval for Polygraph Examinations
- Polygraph Examination
- Polygraph Examination Assistance

470.1.1 Acronyms Table.

470.2 Polygraph Program.
The polygraph program is managed by the polygraph program manager, who reports to the Director of the Forensic and Digital Science Laboratory (FDSL). TIGTA's polygraph program abides by the rules of conduct governed by the National Center for Credibility Assessment (NCCA), which is the Federal center for credibility assessment education, oversight, research, and development. Internal OI standard operating procedures (SOPs) will be consistent with NCCA examiner education and training, continuing education certification, quality assurance programming, and credibility assessment research. OI's SOPs are subject to review by NCCA to ensure consistency with NCCA best practices.

470.2.1 Director Responsibilities. The Director-FDSL is responsible for all polygraph matters connected with TIGTA's polygraph program. The Director has the overall responsibility for the formulation of all policies and requirements relating to the non-technical supervision of the polygraph program and retains the authority to modify any policy. The Director-FDSL has the final authority to deny polygraph examination requests. The Director-FDSL is responsible for granting/revoking certification of all TIGTA polygraph examiners. Additionally, the Director-FDSL will authorize appropriate training, which includes initial certification, continuing education, and developmental

courses and maintain staffing numbers within the program. The Director-FDSL is also responsible for discussing each request with the polygraph program manager.

470.2.2 Program Manager Responsibilities. The program manager is a certified polygraph examiner and is specifically responsible for the administration of the polygraph program. These responsibilities include:

- Final determination of appropriateness to conduct a polygraph examination;
- Justifying final determinations to the Director-FDSL;
- Identifying training opportunities for the polygraph examiners and ensuring all certifications are current; and
- Requisitioning and maintaining necessary equipment and supplies.

The program manager will be specifically responsible for the daily operation of the polygraph program. These responsibilities include:

- Maintaining and preparing reports, statistics, and data relative to polygraph activity;
- Liaising with external polygraph examiners and program managers;
- Conducting briefings and presentations on the polygraph program;
- Conducting polygraph examinations in support of all field elements;
- Providing technical guidance to polygraph examiners;
- Advising the Director-FDSL on matters of examiner proficiency;
- Directing polygraph re-examinations;
- Ensuring all TIGTA polygraph examinations receive a quality control (QC) review;
- Ensuring proper utilization of the polygraph examination;
- Ensuring that correct procedures are executed;
- Ensuring complete and accurate reporting of the examination results;
- Ensuring the monitoring of intern polygraph examiners; and
- Maintaining proficiency in the field to include the knowledge of new techniques, changes in legislation affecting the polygraph profession, and continued familiarity with related fields of study (psychology, physiology, and interrogation).

470.2.3 Polygraph Examiner Responsibilities. Generally, TIGTA-approved certified polygraph examiners, or TIGTA intern polygraph examiners, are authorized to conduct polygraph examinations for TIGTA. Under special circumstances, and with the program manager's concurrence, the Director-FDSL may specifically authorize polygraph examiners from other Federal law enforcement agencies to conduct polygraph examinations for TIGTA; however, every effort will be made to utilize TIGTA polygraph examiners in TIGTA investigations. The responsibilities of polygraph examiners include:

- Assisting with technical expertise in non-jurisdictional cases conducted by other law enforcement entities if approved by the Director-FDSL;

- Approving polygraph interview questions and conducting polygraph examinations in accordance with NCCA guidelines and internal SOPs;
- Providing consultations regarding the appropriateness of conducting a polygraph examination or on other technical or administrative matters related to the polygraph program;
- Providing the case agent with a polygraph examination report;
- Assisting with QC of polygraph examination as needed; and
- Maintaining proficiency in the field to include the knowledge of new techniques, changes in legislation affecting the Polygraph/PDD profession, and continued familiarity with related fields of study (*i.e.,* psychology, physiology, and interrogation, etc.).

470.2.4 Case Agent Responsibilities. The case agent will first contact the program manager and discuss the appropriateness of conducting a polygraph examination. The case agent will complete TIGTA Form OI 7536, *Request for Psychophysiological Detection of Deception Program Services,* and forward through their management chain to obtain the necessary approvals.

470.3 Qualification and Selection of Polygraph Examiners.
OI employees are eligible for selection into the polygraph program and associated training if the employee meets the following standards:

- Possess at least five years of investigative experience;
- Submit to and successfully pass a polygraph security screening examination prior to acceptance for training; and
- Possess a four-year college degree.

The polygraph examiner may be a full-time position or collateral assignment, based upon the needs of the agency. To qualify, the employee must obtain approval from his/her first and second-line supervisors.

470.4 Training and Certification of Polygraph Examiners.
Employees selected for training must successfully complete the PDD Examiner Basic Training Course at the NCCA. Additionally, polygraph examiners must attend a minimum of 80 hours of advanced level or supplementary polygraph/PDD related training every two years. This advanced training will include four hours of refresher countermeasures.

470.4.1 Intern Polygraph Examiner Program. After completion of the NCCA PDD Examiner Basic Training Course, the polygraph examiner must conduct 10-25 monitored polygraph examinations to demonstrate proficiency. Proficiency will be determined by the polygraph program manager and with the concurrence of Director-FDSL.

470.4.2 Polygraph Equipment. OI-issued polygraph equipment will only be used for official polygraph examinations and presentations. Property will be assigned to polygraph examiners and tracked in the Personal Property Module. All property will be returned to the Director-FDSL upon a polygraph examiner's departure from the program.

470.5 When to Request a Polygraph Examination.
In any circumstance where the case agent is unsure of the role or applicability of a polygraph examination, the case agent should contact the polygraph program manager for guidance. Special agents (SAs) should consider the following:

- Polygraph examinations may be used to verify the veracity of information provided by informants, witnesses, sources, and subjects;
- Polygraph examinations may be administered only if the individual participating has been previously interviewed without the presence of polygraph equipment;
- The polygraph examination is to be used as an investigative tool and does not replace a proper and thorough investigation; and
- Polygraph examination results, stemming from a criminal or civil charge, can be submitted as evidence in an employee investigation for the purpose of administrative adjudication.

The polygraph examination will not be used for TIGTA applicant screening or if an individual has a medical condition that would prohibit examination. Other factors will be evaluated to determine suitability of the interviewee.

470.5.1 Factors for Approval. Before requesting a polygraph examination, the case agent will discuss the circumstances of the investigation with a TIGTA polygraph examiner. Factors to consider before requesting a polygraph examination:

- All reasonable investigative efforts been made;
- The polygraph examination is essential to further the investigation;
- There is reasonable cause to believe that the person to be examined is withholding information relevant to the investigation;
- The person to be examined volunteered for the polygraph examination; and
- Whether the polygraph examination will jeopardize any Federal, State, or local prosecution.

470.6 Authorization and Approval for Polygraph Examinations.
Initial approval requests for psychophysiological detection and deception services is approved by the originating Division's Special Agent in Charge (SAC)/Director through the case agent's Assistant Special Agent in Charge/Assistant Director. Final approval is granted by the Director-FDSL, who works in consultation with the polygraph program manager. Additional requests are evaluated and approved on a case-by-case basis.

470.6.1 Requests for Examination. The case agent will complete and submit TIGTA Form OI 7536. The request must include the following information:

- The interviewee's name, date of birth, gender, Individual Taxpayer Identification number, occupation, and position. If an Internal Revenue Service employee is to be examined, include his/her grade, job series, and bargaining unit status. If a minor is to be examined, obtain written parental permission and inform the minor's parents that they may be present during the examination;
- A brief summary of the facts of the case including the involvement of the person to be examined. If monetary theft or bribery occurred, list the amount of money involved;
- Case number and title;
- Evidence associated with the investigation;
- Whether the person to be examined requested the polygraph examination or agreed to submit to a polygraph examination;
- The primary issue to be resolved by the polygraph examiner;
- Confirmation that the person to be examined has agreed to the polygraph examination;
- Confirmation that the employee waives his/her right to union representation (when applicable) during the examination; and
- The city and State where the polygraph examination is to be conducted.

The request will be approved by the case agent's Assistant Special Agent in Charge/Assistant Director and SAC/Director, who will e-mail the approved form to the Director-FDSL. All requests for polygraph examinations shall be documented in the intake/investigation's TIGTA Form OI 6501, *Chronological Case Worksheet*.

470.6.2 Review of Polygraph Examination Requests. TIGTA Form OI 7536 will be reviewed by the program manager. If the request is appropriate, the program manager will forward to the Director-FDSL. If approved, the request will be signed and returned to the case agent.

If it is determined that the polygraph examination is not appropriate, the program manager will return the form to the case agent with a brief explanation for the denial. Requests will be evaluated and returned by the FDSL within three working days of receipt.

470.7 Polygraph Examination.
Once the polygraph examination has been approved, the polygraph examiner will contact the case agent to discuss:

- Overview of the investigation;
- Key factors which need to be resolved;

- Scheduling the polygraph examination; and
- Return information (if applicable) as permitted under 26 U.S.C. § 6103. See Chapter 400, Section 70.3, *Disclosure Authority,* for more information on disclosure authority.

Prior to beginning an examination, the examiner will obtain consent via TIGTA Form OI 7537, *Polygraph Examination Consent*. The polygraph examiner has sole discretion to refuse to conduct or to terminate an examination. Examinations may be visually monitored via a two-way mirror, video cameras, or audio monitors with the consent of the polygraph examiner. All witnesses to a polygraph examination will be identified in the polygraph examiner's report. When practical, the case agent will be available during the examination. The polygraph examiner will provide the case agent with a completed report within five working days.

Polygraph interviews are sensitive and highly technical. National Treasury Employee Union representatives, lawyers, parents, *etc.* are not authorized to be present during polygraph examinations. The interviewee will waive the right to representation during the pretest phase of the polygraph examination. Any interference in the polygraph interview process will result in termination of the examination.

470.8 Polygraph Examination Assistance.
Exceptions to using OI's polygraph examiners include:

- A joint investigation with another agency which has its own polygraph examiners; and
- Exigent circumstances exist which may dictate the services of another Federal agency.

Justification to use another agency polygraph examiner will be documented in Form OI 6501.

470.8.1 Non-TIGTA Polygraph Examinations. If examination assistance is required by a non-TIGTA polygraph examiner, the polygraph program manager will coordinate the request with the assisting Federal agency. The assisting Federal agency will be provided with TIGTA Form OI 7536 and TIGTA Form OI 7537. Once the assisting agency agrees to the examination, the polygraph examiner will coordinate the examination with the case agent consistent with this Section. Outside polygraph examinations will not be conducted without a Memorandum of Understanding in place with the assisting Federal agency.

DATE: April 1, 2021

CHAPTER 400 – INVESTIGATIONS

(400)-480 Insider Threat Program

480.1 Overview.
This Section provides guidance relating to the Office of Investigations (OI) Insider Threat Program (ITP) and contains the following:

480.1.1 Acronyms Table.

480.1.2 Definitions. The following terms are used throughout this Section and are defined below:

Employee – A person employed by, detailed or assigned to, the Internal Revenue Service (IRS) or Treasury Inspector General for Tax Administration (TIGTA); an expert or consultant to the IRS or TIGTA; an industrial or commercial contractor, licensee, certificate holder, or grantee of the IRS or TIGTA, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of the IRS or TIGTA as determined by the appropriate agency head**.**

Insider – Any person with authorized access to any Government resource to include personnel, facilities, information, equipment, networks, or systems.

Insider Threat – The threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

Classified Information – Information that has been determined pursuant to Executive Order 13526, or the Atomic Energy Act of 1954 (42 U.S.C. § 2162), to require protection against unauthorized disclosure and that is marked to indicate its classification status when in documentary form.

480.2 Authority.
The authority set forth in this Section is derived from the following rules, laws, order, and/or regulations:

- 31 USC § 311, *Office of Intelligence Analysis*;
- 31 USC § 312, *Terrorism and Finance Intelligence;*
- 31 U.S.C. 321 (b), *General Authority of the Secretary*;
- IRS Restructuring and Reform Act of 1998 (RRA 98);
- The Inspector General Act of 1978, as amended;
- Executive Order 10450, *Security Requirements for Government Employment;*
- Executive Order 12333, *United States Intelligence Activities;*
- Executive Order 12968, *Access to Classified Information;*
- Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information;*
- Treasury Order 105-20, *Insider Threat Program;*
- Treasury Order 115-01, *Office of the Treasury Inspector General for Tax Administration;* and
- Treasury Directive Publication (TD P) 15-71, *Department of the Treasury Security Manual*.

480.3 Purpose.
The purpose of the ITP is to, deter, detect, and mitigate actions by insiders who either knowingly or unknowingly represent a threat to national security, IRS and TIGTA personnel, facilities, operations and resources. These efforts include conducting insider threat detection and investigative procedures concerning insider threat allegations involving TIGTA and IRS employees, while protecting the privacy, civil rights, and civil liberties of TIGTA and IRS employees.

480.4 Insider Threat Program Responsibilities.
TIGTA has established a systematic means by which relevant information is gathered and disseminated and a specific protocol by which this information is organized and maintained. The responsibilities and activities listed below will facilitate the effective collection and dissemination of criminal intelligence information.

480.4.1 TIGTA Employees. All TIGTA employees have a responsibility to report suspicious behavior to the appropriate management official. Activity on any Department of the Treasury classified or unclassified network, to include portable electronic devices, is subject to monitoring and could be used in a criminal, security, or administrative proceeding.

480.4.2 Deputy Inspector General for Investigations. The Deputy Inspector General for Investigations (DIGI) serves as the senior management official of OI's ITP to ensure accountability and program oversight. The DIGI has established that the ITP is the centralized hub for reporting, analyzing, and responding to insider threat information. The DIGI will establish reporting guidelines for OI personnel to refer relevant insider threat information related to IRS and TIGTA employees to the Special Agent in Charge (SAC)-Special Investigations Unit (SIU).

480.4.3 Assistant Inspector General for Investigations-Special Investigations and Support Directorate. The Assistant Inspector General for Investigations (AIGI)-Special Investigations and Support Directorate serves as the senior management official for the operational activities of the ITP to ensure accountability and program oversight. The AIGI will ensure the SAC-SIU has access to information pertaining to insider threats posed by employees of the IRS, TIGTA, and contractors.

480.4.4 Special Agent in Charge Responsibilities. The SAC-SIU has operational responsibility for the ITP and serves as the primary point of contact for allegations regarding insider threats. His or her designee will coordinate insider threat activities with appropriate external and internal stakeholders, as required, and work in consultation with the SAC-Criminal Intelligence and Counterterrorism Division (CICD) to respond to data calls regarding insider threat activities. The SAC-CICD is responsible for all notifications required by law or Treasury Directive(s). Although the ITP requires coordination from both SIU and CICD, SIU is the sole entity responsible for conducting ITP leads, complaints, or investigations. CICD may, at the request of SIU, provide assistance and de-confliction relative to classified information, as required.

Upon SIU's thorough review of the ITP allegation, the report of investigation or appropriate referral materials will be provided to the appropriate Function Head for review and action. See Section 340. ITP allegations that involve IRS employees or contractors may be deferred by SIU to another division for evaluation. If these referrals result in an investigation, the report of investigation (ROI) must be prepared in accordance with procedures outlined in Section 250.

480.4.5 Chief Information Officer-Office of Information Technology. The Chief Information Officer will proactively promote the use of tools to automate the review of available data sets and transaction logs, and ensure measures are in place and properly updated for identifying suspicious or concerning usage of TIGTA OIT applications.

480.5 Potential Warning Signs of an Insider Threat.
Personal behaviors or factors may indicate an employee intends to act, or is acting against their employer. However, it is important to remember that the presence of some, or even all, of these potential indicators does not mean that an employee is an

insider threat. Similarly, an employee's demonstration of none of the indicators does not guarantee he/she will not pose an insider threat.
The following may be some potential warning signs of an insider threat:

- Anger/revenge-wanting to retaliate against the organization for actual or perceived slights such as lack of recognition, missed promotions, conflict with management or co-workers, or pending furlough;
- Compulsive or destructive behaviors-drug or alcohol dependencies;
- Ego/self-image-"above the rules attitude," subject to flattery or promises of a better job elsewhere; and/or
- Family problems, marital difficulties or other stressors at home.

The following are personal behaviors:

- Unauthorized removal of sensitive/classified information or seeking access to material outside the scope of assigned job duties;
- Working odd hours without approval;
- Taking multiple short unexplained trips, particularly overseas;
- Not reporting continuous and ongoing contacts with foreign nationals or governments;
- Showing interest in project or work outside the employee's job areas;
- Remotely accessing the computer network from home or vacation locations outside of approved work routines; and/or
- Unnecessarily copying manuals, reports, or large volumes of materials.

480.6 Reporting and Documentation of Insider Threat Investigations.
Insider threat investigations may contain classified or sensitive information. Only cleared personnel with a need to know will be granted access to classified and/or sensitive information. Classified and/or sensitive information pertaining to the investigation will be stored in a General Services Administration (GSA)-approved security container. Classified and/or sensitive information **will not** be entered into the Criminal Results Management System (CRIMES), or referenced in CRIMES intake or investigation SharePoint folders.

480.6.1 Intake and Investigation Naming Conventions. CRIMES intakes and investigations involving insider threats will be named in accordance with Section 240. ITP investigations of TIGTA employees must be ghosted to prevent unauthorized access.

480.6.2 Basis Narrative. Allegations regarding insider threats entered into CRIMES shall be general and **will not** contain any classified information.

480.6.3 Chronological Case Worksheet Documentation. The Special agent (SA) will document activities concerning insider threat investigations using TIGTA Form OI 6501, *Chronological Case Worksheet* in generic terms, for example:

- Conducted a review of intelligence report regarding allegation; and
- Met with the Federal Bureau of Investigation (FBI) SA and obtained their report relative to the allegations.

480.6.4 Memorandum of Interview or Activity Documentation. TIGTA Form OI 2028-M, *Memorandum of Interview or Activity* will be used to document investigative activities. In instances where classified information is found that cannot be documented in the Form 2028-M, an annotation shall be made indicating: Several leads were documented in a separate Form 2028-M that were contained in a hard file stored in a secured container.

It may be possible to request from the original classification authority that some or all of a classified document be unclassified for use in ROIs. Consult with CICD for guidance on how to request declassification of classified materials.

480.6.5 Report of Investigation. The TIGTA Form OI 2028R, *Report of Investigation*, will be provided in a hard copy format to the AIGI-Special Investigations and Support Directorate for TIGTA employees or contractors. In consultation with the DIGI, the AIGI will distribute the report to other offices as appropriate for action. See Section 250.

ITP allegations that involve IRS employees or contractors shall be referred in accordance with procedures outlined in Section 250.

480.7 Coordination with External Stakeholders.
The FBI must be advised immediately of any information, regardless of origin, that indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power as required by Section 811 of the Intelligence Authorization Act for Fiscal Year 1995.

To comply with this requirement, the SAC-SIU will ensure that the SAC-CICD is provided with the necessary information to comply with this reporting requirement.

CICD will report all insider threat incidents committed by IRS and TIGTA employees to the Department of the Treasury's Office of Intelligence and Analysis (OIA). SIU, in consultation with CICD as required, will coordinate with OIA and pertinent law enforcement partners on insider threat investigations, incidents, activities, reports and complaints related to IRS employees, TIGTA employees, and contractors. In circumstances where an allegation involves a TIGTA employee, the Office of Mission Support's Personnel Security Office will be consulted, as appropriate.