DATE: July 1, 2020

CHAPTER 500 – INFORMATION TECHNOLOGY

TABLE OF CONTENTS

(500)-140. Enterprise Architecture & IT Security

DATE: July 1, 2019

CHAPTER 500 – INFORMATION TECHNOLOGY

(500)-10 Introduction

This chapter provides an overview of the Office of Information Technology (OIT) to the Treasury Inspector General for Tax Administration (TIGTA). Its purpose is to explain the background, requirements, responsibilities and organizational structure of the function.

10.1 Abbreviations and Acronyms.

Acronyms	Meaning
AO	Authorizing Official
AS	Application Services
ATSC	Atlanta Service Center
CA	Classification Authority
CCB	Change Control Board
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COTS	Commercial Off-The-Shelf
CPIC	Capital Planning and Investment Control
CUI	Controlled Unclassified Information
CS	Cybersecurity Services
DLP	Data Loss Prevention
EA	Enterprise Architecture
ES	Enterprise Services
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FITARA	Federal Information Technology Acquisition Reform Act
FMFIA	Federal Managers Financial Integrity Act of 1982
GPRA	Government Performance and Results Act of 1993
HTML	Hypertext Markup Language
IM	Instant Messaging
IO	Information Owner
ISSO	Information System Security Officer
IT	Information Technology
ITMRA	Information Technology Management Reform Act of 1996 (Clinger-Cohen Act)
ITSS	IT Solution Services
IS	Infrastructure Services
MCC	Martinsburg Computing Center
MFP	Multifunction Printer
MP	Media Protection
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OGE	Office of Government Ethics
OIT	Office of Information Technology
PII	Personally Identifiable Information
POA&Ms	Plans of Action and Milestones
SD	Service Desk

Acronyms	Meaning
SBU	Sensitive But Unclassified
SNN	Social Security Number
SOP	Standard Operating Procedure
SQL	Structured Query Language
TCSIRC	Treasury Computer Security Incident Response Center
TIGTA	Treasury Inspector General For Tax Administration
TIN	TIGTA Information Network
TNet	Treasury Network System
TO	Treasury Order
TRB	Technical Review Board
VPN	Virtual Private Network
WS	Web Solutions

10.2 Background.

The Office of Information Technology (OIT) provides cost-effective, timely Information Technology (IT) products and services that permit successful completion of TIGTA's strategic goals while meeting legislative mandates. OIT has responsibility for data and system administration of the network, technology standards, security assurances, telecommunication deployment, and integrated application development. It is OIT's responsibility for ensuring compliance with federal statutory, legislative and regulatory requirements governing confidentiality, integrity and availability of TIGTA's IT systems, services and data.

10.3 Legislative Authority and Responsibility Relating to OIT.

- **Clinger Cohen Act of 1996.** The Act requires affected Federal agencies to designate a CIO and to put in place systems for effectively applying performance and results-based management principles to the development, acquisition and maintenance of information technology systems.
- **Federal Information Technology Acquisition Reform Act (FITARA).** This Act requires the heads departmental offices to ensure that their respective CIOs have a significant role in IT decisions, including annual and multi-year planning, programming, budgeting, execution, reporting, management, governance, and oversight functions. FITARA augments the Clinger-Cohen Act of 1996 to address concerns about waste and ineffectiveness in federal IT investments.
- **Federal Managers' Financial Integrity Act of 1982 (FMFIA).** The FMFIA amends the Accounting and Auditing Act of 1950 and requires each executive Federal agency to establish and maintain internal accounting and administrative controls in accordance with standards prescribed by the Comptroller General of the United States.

DATE: July 1, 2019

CHAPTER 500 – OFFICE OF INFORMATION TECHNOLOGY

(500)-20 Organizational Roles and Responsibilities

20.1 Responsibilities.
The Office of Information Technology (OIT) provides cost-effective, timely Information Technology (IT) products and services that permit successful completion of TIGTA's strategic goals while meeting legislative mandates. OIT has responsibility for data and system administration of the network, technology standards, security assurances, telecommunication deployment, and integrated application development. It is OIT's responsibility for ensuring compliance with federal statutory, legislative and regulatory requirements governing confidentiality, integrity and availability of TIGTA's IT systems, services and data.

20.1.1 Chief Information Officer. The Chief Information Officer (CIO) position reports directly to the Inspector General (IG). The CIO oversees day-to-day Information Technology (IT) operations of TIGTA and provides strategic and operational oversight for IT services and solutions that align with TIGTA's mission.

20.1.2 Organizational Structure. The OIT organizational structure is composed of four directorates: Cybersecurity Services (CS); Enterprise Services (ES); IT Solution Services (ITSS); and Infrastructure Services (IS). All four directorates report to the CIO and have overall responsibility for the program areas denoted below:

- **Cybersecurity Services (CS)** – Responsible for ensuring compliance with federal statutory, legislative, and regulatory requirements and directives governing confidentiality, integrity and availability of TIGTA's systems, services and data. Cybersecurity manages TIGTA's IT Security Program in accordance with the Federal Information Security Management Act (FISMA). This group is also responsible for mitigating risk related to internal and external data breaches and cyber attacks.

- **Enterprise Services (ES)**

  Governance – Manages the leadership, management, oversight, and direction necessary for the development and implementation of TIGTA's standards and technology infrastructure across the enterprise. It is focused on providing consistent, efficient, flexible and sustainable solutions intended to improve the quality of information systems, products and services. ES is also responsible for improving partnership, transparency, and communication between OIT and the other TIGTA Functional Units. It is responsible for ensuring that TIGTA's architecture falls within the Federal Enterprise Architecture guidelines and adheres to industry best practices to the extent that it can without sacrificing mission, security and privacy exigencies.

Service Desk – Manages TIGTA's Service Desk primarily for technology assistance and problem management associated with OIT components and services for the end-user. TIGTA's Service Desk serves as the single point of contact for all matters concerning IT related incidents, inquiries and service requests. The Service Desk also serves as the initial point of contact for several Office of Mission Support (OMS) program areas (*e.g.*, facilities*)*. Such non-IT related Service Desk tickets are forwarded appropriately for action by OMS.

- **IT Solution Services (ITSS)**

  Application Services – Manages day-to-day operations and maintenance of TIGTA end-user devices provisioned by OIT. The group is also responsible for patch management and provides elevated support activities for service desk as well as wireless and removable media encryption services.

  Web Solutions – Manages software development, design, test, implementation, and maintenance activities. The group has principal responsibility for implementing/developing, testing, delivering and maintaining TIGTA's business applications to fulfill its business needs. The group is also responsible for hosting and maintaining a variety of Commercial Off -The-Shelf (COTS) products as determined through specific Business Unit needs. These responsibilities include database administration, systems administration, support of production versions of customized software, level-2 customer support as well as user and system technical writing. This group also manages all internal development and postings for TIGTA's Intranet/Internet site.

- **Infrastructure Services (IS)**

  Server Management – Manages the day-to-day operations and maintenance for TIGTA's server infrastructure. This includes:
  - Plans, designs, implements and maintains physical server configurations, virtual server configurations and storage (SAN) environments.
  - Maintains and supports the base server hardware and server operating system for all TIGTA systems. This includes operating system updates, patching and troubleshooting.
  - Manages the Windows Server Operating System, Red Hat Linux operating system and VMWare ESX server.
  - Installs, supports and manages Microsoft Active Directory services including AD design, advanced configurations and user and group management.
  - Collaborates with system owners to size infrastructure for new applications, install and maintain those systems as configured and implement server backups.

- Assists system owners as needed with server configuration and contingency plans.
- Manages infrastructure servers for email, including Microsoft Exchange software and all related configurations. Manages email archiving solutions and configurations.
- Manages the Symantec Endpoint Protection (SEP) infrastructure and client for TIGTA servers.
- Manages infrastructure servers for mobile device management.

Telecom Services – Manages all of TIGTA's components providing Wide Area Networking capabilities through the Treasury Network (TNet) and all interactions with the Treasury networks and telecommunications program office. This group is also responsible for Local Area Network office connectivity and network connectivity to other federal agencies and all other entities outside of TIGTA.

Data Services – Responsible for managing and supporting the TIGTA Data Center Warehouse (DCW), which serves as a centralized data repository for federal tax information and administrative data. This includes transforming, loading, and maintaining of IRS tax administration data necessary to support TIGTA's tax administration oversight activities. Data Services also develops and maintains query tools to facilitate the analysis of IRS tax administration data.

20.2 TIGTA Information Network.

The TIGTA Information Network (TIN) or TIGTANet consists of approximately 61 sites geographically dispersed across the contiguous United States, Alaska, Hawaii and Puerto Rico. Each site has laptops that have access to the TIGTA Microsoft Active Directory domain. This backbone, using a combination of physical and virtual configurations, provides employees with site-licensed software, access to file storage on servers, e-mail and mobile services. The TIN also allows access by authorized personnel to other computer systems and applications located in two central locations; the Martinsburg Computing Center (MCC) and the Atlanta Service Center (ATSC). These two facilities serve as host to the majority of TIGTA's owned and shared infrastructure and computing services. In addition, access to the Internet and Intranet is provided, as is access to IRS and other Treasury systems and resources via the Treasury Network System (TNet).

DATE: April 1, 2018

CHAPTER 500 – INFORMATION TECHNOLOGY

(500)-30 TIGTA Wide Print, Copy, Scan and Fax Policy

30.1 Introduction.
This section provides the policies and procedures for the Treasury Inspector General for Tax Administration (TIGTA) printing, copying, scanning, faxing, and paper use. The Office of Information Technology (OIT) administers this program, including the purchase and deployment of all printing devices in a manner that incorporates efficient spending, promotes effective operational success, complies with federal guidance, and provides services in an environmentally responsible manner.

This policy will be reviewed on an annual basis to ensure its continued accuracy.

30.2 Authorities.
This policy supports a number of executive and legislative initiatives to promote efficient utilization, purchasing, and deployment of print devices:

a. Executive Orders 13101, 13693, 13589
b. OMB Circular A-130
c. GSA Bulletins B-37, B-34
d. Department of the Treasury's Sustainability Plan

30.3 Types & Distribution.
TIGTA utilizes the following types of devices:

- Multifunction Printer (MFP): A MFP is an all-in-one multi-functional printer/copier/scanner/fax that is on the TIGTA network users print via mapping to a defined print queue. Print queues are hosted on network attached print servers in each TIGTA location. There are two MFP models in TIGTA. One device is suited for small to mid-sized workloads and the other device is more suitable for higher volume needs. Selected models possess full functionality and feature easy-to-use touch screen interfaces. The devices work with smart cards (HSPD-12 cards) allowing the end-user to scan documents directly to their TIGTA network drive or their TIGTA e-mail account.

- Traditional Laser Printers: Traditional laser printers may be deployed by OIT in a TIGTA environment, on a limited basis. These printers will be used to fill utility purposes where print functionality is needed but a MFP is not suitable. There may be a limited number of laser printers available for "convenience" purposes and assigned to specific individuals. All requests for convenience printers must be approved by the function approving officer and the CIO prior to fulfillment.

- Telework Printers and (mobile) Scanners: These devices are not connected directly to the TIGTA network. These devices are distributed on an as needed

basis. Specifications of these devices may vary due to market availability and differences among manufacturers.

All TIGTA offices are configured with at least two MFPs for redundancy of all features – print, copy, scan, and fax. This allows for continuity of local business operations if one of the MFPs go out of service.

TIGTA OIT is the sole approver of ALL print and multi-function devices, to include telework and specialty printers and mobile scanners. Use of non-TIGTA OIT approved devices, including personal desktop printers, legacy printers, copiers, and scanners is expressly prohibited. This benefits TIGTA by maintaining a secure environment, and lowering energy consumption, equipment volume and maintenance, supplies, and vendor-related service costs.

All TIGTA employees are responsible for treating devices as TIGTA personal property in accordance with Chapter (600)-100 – Personnel Property Management Program.

30.4 Security.
All MFPs feature smart card (HSPD-12 cards) readers. These readers can be used to authenticate to the TIGTA network and securely scan documents from the MFP directly to a user's network drive or a TIGTA e-mail account.

Secure printing is available via "pin printing" where users select a four-digit pin code prior to sending a print job to the MFP. When the user physically arrives at the device to retrieve the print job, the selected pin is entered and the print process will begin. All employees are encouraged to use this feature when printing PII and any sensitive or confidential information.

Under no circumstances should TIGTA employees attempt to relocate MFPs on their own. All requests to physically move MFPs should be submitted to OIT who will coordinate the relocation with the Office of Mission Support (OMS) and onsite personnel as appropriate. It is OK to slightly move the MFPs to remove paper jams and to allow for temporary movement for cleaning carpets and replacement of carpet tiles.

30.5 Default Print Settings.
In accordance with Treasury, the Office Management and Budget (OMB) guidance and directives and in an effort to achieve energy savings, reduce paper cost create less waste, and reduce environmental impact, OIT has configured all eligible devices as follows:

- Duplex or double-sided printing – All devices are configured to print in duplex mode as the default. Duplex printing has the potential to reduce paper consumption by half when compared to single-sided printing and thus reduces costs and environmental impacts.

- Grayscale or monochrome printing – All devices are configured to print and copy in grayscale. Color pages cost more to produce and this step reduces the associated costs while providing the flexibility to print in color. A single word or phrase on a page (e.g. a web link or email address) displayed in color counts as a color page which incurs a higher charge. End-users may override the grayscale setting for print jobs or copies but should only do so when color printing is absolutely necessary.

TIGTA employees should follow the below recommendations when possible:

- Be prudent when deciding to print versus leaving something in electronic format for reference. Do not unnecessarily print e-mails and documents.
- Create and distribute documents electronically – post to a SharePoint site or distribute via e-mail. Provide printed copies only as necessary.
- Review and edit draft documents on-screen rather than on paper.
- Use electronic/digital signatures for approving documents whenever possible.
- Use print preview to ensure your document will print correctly.
- Print only the number of copies required.
- Adjust page layout (margins) and text size to minimize use of paper.

30.6 Purchasing and Replacing.

OIT is responsible for controlling the purchase of all print devices. The following must be taken into consideration:

1. All new printers, copiers, and multifunctional devices must meet current Energy Star requirements.
2. In those cases, where Electronic Product Environmental Assessment Tool (EPEAT) criteria apply, new devices must meet the silver standard or higher.
3. TIGTA must use paper with a post-consumer fiber content of 30 percent or greater. Minimal exceptions will be granted for the use of paper for special displays, and other formal events. The main target of this policy is 8½" x 11" sized paper. This is the most commonly utilized paper size. Alternative sizes may be included as practical and as the print device permits (e.g. legal sized paper (8.5" x 14").

30.7 Managed Print Services.

TIGTA MFPs are managed under a services contract with a commercial vendor. All hardware support and consumable fulfillment are included as part of our agreement. Toner levels and other consumables are monitored and as an item (e.g., toner) begins to reach agreed upon thresholds, a replacement will be automatically shipped to the appropriate office. Toner is shipped on a "just-in-time" fashion and should arrive days or even weeks before it is actually needed.

If a low toner condition is being reported and the office has not yet received a replacement cartridge, employees can e-mail the support address listed on the sticker on the front chassis of the MFP. Provide the serial number listed on the support sticker and state what specific toner color is needed. The cartridges should arrive within 48

hours of order receipt. Field offices will replace their own toner. In NHQ, users can submit a service desk ticket when toner begins to impact print quality and IT Customer Support will replace the cartridge.

If a TIGTA printer requires maintenance, users must submit a TIGTA service desk ticket for initial troubleshooting purposes. OIT will work with the user to diagnose and in many cases resolve the issue. If a physical repair is required due to equipment failure OIT will assist the site in opening a service ticket with the vendor. Most repairs are expected to be completed in 24-48 hours.

Paper levels are NOT monitored by the service contractor. This is the responsibility of local TIGTA staff. All TIGTA personnel should be familiar with the procedure to add/ replace paper and toner.

Toner and paper for traditional laser printers, to include telework printers, is budgeted at the functional level.

30.8 Limitations on What May be Copied.
Multiple copies of material protected by United States Copyright Laws cannot be legally reproduced without express, written consent of the copyright owner. All TIGTA employees are responsible for complying with copyright restrictions.

In addition, multiple reproductions of standard forms available through websites or supply orders should be minimized, and if possible, completely avoided.

When copying currency, the currency must be reduced to 70 percent of the original size or more than one and one half of the original size, as required by Title 31, CFR, Section 411.

30.9 FAX Services.
Each MFP at TIGTA is a FAX capable device. The MFP, if connected to an analog line, can both send and receive traditional faxes. MFPs connected to FAX lines should have a sticker on the printer chassis indicating the FAX number, and also will have a FAX option on the main menu of the touch screen interface. If the MFP you are using has neither of those then it is not enabled for FAX services.

The MFPs can only be configured for fax services in an office where the phone lines are NOT owned by Internal Revenue Service (IRS). IRS policy prohibits the connection of MFPs to their phone systems. In offices where TIGTA uses IRS infrastructure, we will comply with the IRS policy. Contact the Service Desk if you have a need to configure the multifunction printer for fax.

When faxing documents, TIGTA users must monitor transmittals closely to ensure information is not inappropriately transmitted or received. For example: call the person to whom the facsimile is intended to alert them to standby to receive the transmission.

Additionally, all TIGTA employees must abide by Chapter (500) 140-4 Sensitive Information Protection Policy.

30.10 Inventory Reconciliation.

On or about January 1 of every year, OIT will certify that the inventory list is correct. Any missing property will be reported in accordance with Chapter (600)-100 – Personnel Property Management Program.

DATE: April 01, 2019

CHAPTER 500 – INFORMATION TECHNOLOGY

(500)-40. TIGTA Enterprise Systems Backup Tape Purpose and Retention Policy

40.1 Introduction.
This section establishes the purpose and retention policy for Treasury Inspector General for Tax Administration (TIGTA) enterprise system backup tapes. The Office of Information Technology (OIT) administers this program, including the purchase and deployment of all backup software/hardware and tape media. OIT also manages the offsite storage of the tape media.

40.2 Authorities.
General Records Schedule Number 3.2 - DAA-GRS-2013-0006

- See Section 4 on page 2 of Review Version 4/29/2013.

40.3 Backup Tape Purpose.
Backup tapes created as part of the TIGTA enterprise system backup processes are solely for restoring servers in the event of a catastrophic hardware failure. In the event of a catastrophic server failure, the tapes will be used by the Server Team to restore the server back to the point in time the backups were successfully completed. See SOP-08.12 for the backup tape creation schedule.

Data on the tapes includes, but is not limited to, all TIGTA servers including CRIMES, TeamMate, and SQL Server.

40.4 Backup Tape Retention Policy.
Once tapes are created as part of the backup processes, they will be retained for no longer than six months. When backup tapes for the seventh month are created and verified, the backup tapes for month one are retrieved from the offsite storage location and reused (and overwritten) or destroyed, depending on the lifecycle of the tapes.

40.5 Exceptions.
Exceptions to the retention policy described above include the following:

- Splunk data will be backed up to dedicated tapes and, on a quarterly basis, sent offsite. The Splunk tapes will be retained for six years.
- Data Center Warehouse d ata. See SOP-8.11.

This policy will be reviewed annually.

DATE: April 1, 2018

CHAPTER 500 – INFORMATION TECHNOLOGY

(500)-60 Instant Messaging

60.1 Overview.
The current TIGTA implementation of Instant Messaging (IM) is the Microsoft branded Skype for Business service. The tool provides TIGTA users support for their official work duties by providing: application/desktop sharing capabilities, conducting virtual meetings, white-boarding, presence, and exchange of instant messages. The capability can also support teleconferencing and videoconferencing but is not currently implemented. The TIGTA IM client starts up automatically when users log on to their laptop.

60.2 Acceptable Use.
One of the benefits of IM and collaboration is the ability for colleagues and managers to know where colleagues/subordinates are so there is little/no time wasted obtaining status, making an assignment, verifying user's location/safety in case of an emergency, etc. TIGTA OIT encourages users to make their presence or location known. Omitting the user's location or appearing to be in the one location when in another is not an appropriate use of the tool and undermines its value.

Current TIGTA policy regarding instant messages is that they are not stored or retained. When the conversation ends and the session is closed or users log off, the contents are lost and cannot be retrieved. Storing IM may also discourage its use as an informal means of communicating. IM should only be used for informal business communications and collaborations, and not to engage in discussions regarding policy matters, business decisions, or documentation of other mission-critical functions.

TIGTA's current implementation of IM allows for communications within the TIGTA network only and will not work for communications outside of TIGTA.

60.3 Record Management Requirements for IM Solution.
TIGTA is not required by law or regulation to configure its IM system to capture and store transcripts of all traffic. The content of the majority of instant messages are expected to be informal, transitory, and logistical. Because instant messaging content will generally be informal and transitory, most will not meet the definition of "records" that must be retained. In an event an instant message is created to set agency policies or make agency decisions, or if the IM otherwise meets the definition of a record for purposes of the Federal Records Act, the content of such messages must be preserved. A record can be made by creating a memo or an e-mail if the engaged parties believe that is necessary.

Other instant messages that you must preserve include those that:

- Contain information subject to a litigation hold;

- Relate to a Congressional inquiry; and/or
- Relate to a Freedom of Information Act request.

For additional information about record management requirements visit **Chapter (600)-110 – Records Management.**

DATE: January 1, 2020

CHAPTER 500 – INFORMATION TECHNOLOGY

(500)-70. E-mail Retention Policy

70.1 Introduction.
This section establishes the retention policy for the Treasury Inspector General for Tax Administration's (TIGTA) enterprise e-mail environment. E-mail retention includes a combination of active mailbox and archived e-mail content. Retention also includes both onsite (active) and offsite retention at the National Archives and Records Administration (NARA) where applicable.

70.2 Authorities.
- 36 CFR Chapter XII, Subpart B – Agency Records Management Responsibilities
- 36 CFR Chapter XII, Part 1236 – Electronic Records Management
- NARA GRS 6.1, E-mail Managed Under a Capstone Approach
- NARA Bulletin 2014-06, Guidance on Managing E-mail Records
- NARA Bulletin 2013-02, Guidance on a New Approach to Managing E-mail Records
- OMB M-12-18, Managing Government Records Directive
- Treasury Directive 80-07, Department of Treasury E-mail Management
- Treasury Directive Publication 80-07, E-mail Management
- TIGTA Memorandum #18-07, Litigation Holds

70.3 Scope.
This policy applies to all TIGTA employees (contractors, volunteers, detailees, and interns) who use TIGTA's e-mail system, to include Capstone and Non-Capstone individuals.

70.4 Capstone Approach Requirements
Directive M-12-18 Managing Government Records requires Federal agencies to manage both permanent and temporary e-mail records in an electronically accessible format. TIGTA adopts as a matter of policy the NARA-developed Capstone approach for managing e-mail records, as described in NARA Bulletin 2013-02, which is a more simplified and automated approach rather than a print and file system or record management application. This policy applies to e-mails received after January 1, 2018.

The Capstone approach allows TIGTA to categorize and schedule e-mail based on the position of the e-mail account holder and designate those e-mail accounts as permanent. All other e-mail accounts are designated temporary and are governed by their respective records schedules. As defined below, the Capstone designation is applied to a small subset of TIGTA senior leadership positions.

70.4 Responsibilities.
Office of Information Technology (OIT) – The OIT Administers this program, including the purchase and deployment of all Messaging related software and hardware. OIT also manages the daily operation of the internal electronic mail subsystem and it is responsible for managing the e-mail retention schedules in accordance with this policy.

TIGTA's Records Management Officer (RMO) – The RMO manages the Capstone program for policy, end-user training, compliance responsibilities, and communicating with OIT of individuals who fall under the Capstone approach.

Office of Chief Counsel (OCC) – The Office of Chief Counsel operates as a contact point for records sought from TIGTA by parties in litigation through discovery requests such as requests for production of documents. While the Office of Chief Counsel operates as a contact point, including, determining the scope of legal holds and searches and coordinating with OIT to identify, preserve, and collect electronically-stored information that may be responsive, the TIGTA function that maintains the responsive records is responsible for gathering and reviewing the records sought to determine relevancy and possible assertion of privilege (e.g., informant privilege). The Office of Chief Counsel maintains a list of active litigation hold notices.

Office of Mission Support, Leadership & Human Capital (L&HC) – L&HC provides current rosters of SES employees in both the position of record and acting capacities upon regular request from the RMO.

Account holders – All TIGTA employees (contractors, volunteers, detailees, and interns) who use TIGTA's e-mail system, to include Capstone and Non-Capstone individuals will appropriately manage e-mail content as aided by this policy and will treat records as described in (600)-110 – Records Management and Treasury Department Publication (TD P) 80-05. Additionally, all TIGTA employees will be responsible for completing *Records Management Employees and Contractor* training on an annual basis. The training will be handled like all other TIGTA mandatory training. This course will also be added to the list of required training for all newly hired TIGTA employees.

For any records management questions, please contact TIGTA's Records Management Officer at *TIGTA OMS Records Management. For any technical questions about how the new Capstone process will apply to your emails, please contact the Service Desk by submitting a ticket online.

70.5 Capstone Approach Retention Procedures.
Capstone Officials – Capstone officials within TIGTA include the Inspector General; all members the Senior Executive Service; and anyone acting on a temporary basis in one of these positons for more than 60 days will also be considered a Capstone official for the duration of their acting role. The TIGTA RMO maintains an official list of capstone officials' e-mail accounts, including acting assignments.

Non-Capstone Officials – All other users not listed as a Capstone position (including contractor, volunteer, detailees, and interns) are non-Capstone officials.

E-mail retention procedures for all TIGTA employees is summarized in the following chart:

Role	Onsite Retention	Disposition
Capstone Officials	E-mail records will remain in the user's e-mail "Inbox" for one year. After one year, items will be moved to archive in Enterprise Vault and will be available for a total of 15 years between active Inbox and archive storage.	**Permanent** – Records will be transferred to NARA for permanent retention after 15 years, or declassification review, whichever is later. After transfer, records will be permanently deleted from the active (onsite) TIGTA e-mail system.
Non-Capstone Positions	E-mail records will remain in the user's e-mail "Inbox" for one year. After one year, items will be moved to archive in Enterprise Vault and will be available for a total of 15 years between active Inbox and archive storage.	**Temporary** – Records will be permanently deleted from the active (onsite) TIGTA e-mail system after 15 years unless additional retention is required for business use (*e.g.*, litigation hold).

70.6 Encrypted E-mail.
E-mail that is archived in encrypted format must be decrypted prior to transfer to NARA. This includes deactivation of passwords or other forms of file level encryption that would impede access to record data. OIT will work with the business units to define a process, preferably automated, to decrypt applicable items prior to transmission to NARA.

70.7 Litigation Holds.
A litigation hold notice is issued to inform the recipient of impending or actual litigation, the legal obligation to preserve paper records and/or Electronically Stored Information (ESI), including e-mail, related to the litigation, and the need to provide information in response to the notice. Once paper records and/or ESI subject to a litigation hold have been identified and located, they must be preserved to ensure that they are not destroyed or altered, until the litigation hold has been lifted. As a result, all applicable record retention schedules **are suspended** until such time as the litigation hold has been released to ensure certain records are collected and preserved for use in litigation. Generally, ESI must be maintained in its native format. The responsibilities regarding litigation holds are identified in TIGTA Memorandum 18-07, Litigation Holds, and TIGTA Operations Manual, Chapter (700)-90.3. Questions concerning the appropriate manner to preserve ESI should be directed to TIGTA Counsel.

70.8 Transmitting Date to NARA.
The TIGTA OIT will be responsible for transmitting e-mail records to NARA in accordance with the record retention schedule. The process to transmit this data has not yet been defined. Capstone took effect January 1, 2018, so the first archive data is due to be transmitted to NARA around January 1, 2033. This policy will be updated as the process to transmit data is defined.

(500)-100 Office of Information Technology Training

100.1 Training Policy.
The Office of Information Technology (OIT) is committed to providing training to all levels of the OIT organization to keep in step with the rapidly changing pace of technology. Training activities will be accomplished within the context of operational priorities and budgetary constraints. The Chief Information Officer (CIO) will allocate a training budget to the OIT Directors at the start of each fiscal year. The Management Analyst (MA) and the CIO will coordinate with the Directors to identify training issues resulting from new or updated technology initiatives (*e.g.*, implementing a new software package).

100.2 Training Coordination.
Directors will act as the training coordinator for their respective sections. The Directors may delegate assignment of specific training and development of individual training plans to the respective Assistant Directors within their Directorate. The CIO will act as training coordinator for the CIO's immediate staff and also coordinate overall training activities for the Directors. The MA will function as the liaison with the Treasury Inspector General for Tax Administration (TIGTA) National Training Coordinator representing OIT on training related issues.

100.3 Skills Assessment.
At the start of each fiscal year, Directors will develop an inventory of the skills necessary to accomplish their Directorate's responsibilities. During performance reviews, the Assistant Directors will match the knowledge, skills, and abilities of their staffs against the inventory, and document each individual's training needs and the specific training plans developed for individual employees, as appropriate.

100.4 Training Plan.
The Directors and Assistant Directors will review the aggregate training needs and develop a training plan for their respective Directorates. Directors will monitor the accomplishment of their section's training plan throughout the year. The use of an individual development plan (IDP) is optional for staff performing at a satisfactory level. A formal Performance Improvement Plan (PIP) lasting at least 90 days is mandatory for any staff member before they can be rated "Unacceptable" on any critical element. Before placing anyone on a PIP, the manager should contact Employee Relations in the Office of Mission Support and the Office of Chief Counsel

After the mid-year performance reviews, Directors will revalidate the skills inventory for their sections, make adjustments to the training plan, and submit to the CIO unfunded and projected training needs exceeding funds available to the Director for possible additional funding or for planning the following year's budget request.

Directors and Assistant Directors must consider the rapidly changing nature of information technology. Care and consideration must be given to current technology and the pathway to future technologies. IT professionals must stay abreast of developments that impact not only their specific areas of responsibility but those areas where technological changes impact their areas of expertise and responsibility in an indirect or tangential fashion. While specific roles require specific knowledge and periodic updates to skills, TIGTA IT professionals are required to be current in their respective areas and those areas that have an impact on their primary area of responsibility.

Each member of the OIT staff is required to participate in a minimum of six hours of Continuing Professional Education (CPE) technology related training annually. This training should be based on required knowledge, skills, and competencies and should be linked to TIGTA's strategic plan and goals. Additionally, this training should be conducted by authorized sources and offer certification of completion. These can include, but are not limited to, vendor training (*e.g.*, Microsoft, CISCO, etc.) or other organizations authorized to provide stand-up or online training for the topic (*e.g.*, Learning Tree.) Mandatory training for all TIGTA personnel is not a substitute for this CPE.

100.5 Training Requests.
Employees seeking to attend individual training offered either by government agencies or non-government sources are to submit a completed SF-182 (Authorization, Agreement and Certification of Training) via the Treasury Learning Management System (TLMS).

Training requests should be approved only for training that supports the TIGTA mission and performance goals. The SF-182 approving officials must be as follows:

1. First Line Manager
2. OIT Management Analyst
3. Purchase Card Holder
4. Auto Approver
5. Auto Approver

Employees who attend training without managerial approval may become personally liable for that training expense.

For information on TIGTA's training policy please see Chapter (600)-70.19, TIGTA Training in the TIGTA Operations Manual.

DATE: July 1, 2020

CHAPTER 500 – INFORMATION TECHNOLOGY

TABLE OF CONTENTS

DATE: April 1, 2020

CHAPTER 500 – INFORMATION TECHNOLOGY

140.1 Security Controls

140.1.1 Overview.
This Information Technology (IT) Security policy ensures the Treasury Inspector General for Tax Administration's (TIGTA) information systems comply with applicable security requirements mandated by Federal standards and Treasury policies in accordance with the Federal Information Security Modernization Act (FISMA) of 2014. Complying with security requirements is critical in ensuring the integrity, availability, and confidentiality of TIGTA's information and information systems components. The FISMA act of 2014 requires each Agency and Bureau to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective organization. Accordingly, this policy provides requirements across key areas to be addressed in the TIGTA's information security programs. The evaluations identify TIGTA FISMA systems' security vulnerabilities and associated control weaknesses. This policy clarifies Federal and Treasury security requirements, adopts them to TIGTA's specific information systems, and imposes additional TIGTA specific requirements, when necessary.

TIGTA's information system, subsystems, and associated systems are rated as moderate impact level systems according to Federal Information Processing Standard (FIPS) Publication 199 - Standards for Security Categorization of Federal Information and Information Systems ratings. The FISMA of 2014 directs the designation of security impact levels based on FIPS 199 standards.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, recommends Federal agencies and bureaus develop a formal, documented security policy so that applicable security controls are effectively implemented and maintained on IT systems within the organization.

140.1.2 Purpose and Management Commitment.
This policy represents the commitment of TIGTA to ensuring that all applicable security requirements are appropriately defined and implemented, in order to comply with Federal standards and Treasury policies. This goal of this commitment is to protect TIGTA against intentional or unintentional acts that could negatively impact the confidentiality, integrity, and availability of TIGTA's systems and data.

140.1.3 Scope.
This policy applies to all TIGTA personnel, including contractors and vendors, and IT system components and technology within the TIGTA operating environment or connected to the TIGTA information infrastructure.

140.1.4 Roles and Responsibilities.
Outlined below are the roles and responsibilities associated with the TIGTA information security program.

140.1.4.1 Chief Information Officer (CIO). TIGTA's CIO oversees the IT security program and advises leadership on significant issues related to the security program. The CIO confirms that an acceptable risk posture of TIGTA systems is accomplished in accordance with applicable security controls established by Treasury and other Federal policy and guidance.

The CIO ensures security weaknesses are correctly identified and appropriately prioritized within TIGTA's Plans of Action and Milestones (POA&Ms) submissions.

140.1.4.2 Authorizing Official (AO). The AO is responsible for the overall management of TIGTA's IT security program. The AO allocates resources to ensure proper identification, implementation, and assessment of common security controls on TIGTA IT systems. The AO ensures each TIGTA IT system undergoes regular assessments in accordance with established timeframes. The AO reviews the results of continuous monitoring efforts and authorizes continued operations if the risks of the findings are acceptable and the appropriate POA&Ms are created. The AO ensures system authorizations are conducted in accordance with Treasury and TIGTA defined policy and frequencies.

140.1.4.3 System Owner. System owners are the TIGTA managers responsible for the overall procurement, development, integration, modification, operation, and maintenance of TIGTA's information systems. They rely on the assistance and advice of the TIGTA Chief Information Security Officer (CISO), IT Assessment and Authorizations (A&A) Team, Information System Security Officers (ISSO), system administrators, and other IT staff in the implementation of security responsibilities and maintenance of security requirements. System owners ensure system-level POA&Ms are created in response to any security vulnerabilities discovered and ensure corrective actions are implemented in accordance with Treasury and TIGTA policies.

140.1.4.4 Chief Information Security Officer. The CISO develops TIGTA's cyber security program and serves as the central point of contact to ensure TIGTA's security policies and procedures comply with Federal and Treasury mandates. The CISO ensures the CIO and AO are informed of TIGTA's overall cyber security status and risk posture. The CISO ensures that system security plans and other security related documents are developed, implemented, and reviewed in accordance with TIGTA policy. The CISO is responsible for any AO approved actions listed in the AO delegation representative memorandum. The CISO confirms that an ISSO is assigned for each TIGTA IT system.

The CISO oversees annual IT system security assessments, to include technical control testing and updated risk analyses, in compliance with TIGTA policy and applicable

guidance. The CISO monitors the status of TIGTA POA&Ms on all cyber security weaknesses, and tracks milestones and allocation of resources for remediation through completion. The CISO reports the results of continuous monitoring to the AO and other TIGTA officials as appropriate to request Authority to Operate (ATO) on TIGTA's FISMA systems.

The CISO works with the Contracting Officer's Representatives (CORs) and procurement office to ensure IT security requirements are fully addressed in TIGTA IT procurements, business cases and budget submissions. The CISO works with CORs to ensure that contractors comply with this security policy and pursues appropriate action for noncompliance.

140.1.4.5 Assessment and Authorizations Team. TIGTA A&A Team, led by the CISO, is responsible for providing oversight and guidance to ISSOs, IT staff, and the TIGTA workforce in complying with TIGTA's cyber security program. The A&A team facilitates the implementation of security controls within TIGTA, on behalf of the CISO, and monitors TIGTA IT systems to ensure compliance. The A&A team guides the development of system security plans and other security related documents. The A&A team verifies that controls found in this policy have been implemented and documented appropriately. The A&A team monitors the security operations of TIGTA information systems, including physical security, personnel security, security training and workforce awareness; and reports any inconsistencies to the CISO. The A&A team is responsible for providing incident response reporting services for TIGTA. These include receiving information on possible incidents, investigating them, and taking action to ensure any incidents are reported to the Treasury Computer Security Incident Response Center/Global Security Operations Center (CSIRC/GSOC) within the required time period.

140.1.4.6 Security Control Assessor (SCA). The SCA is responsible for continuous monitoring of the security controls of TIGTA IT system. The SCA is in a position that is independent from the persons directly responsible for the development and day-to-day operation of the system. The SCA should also be independent from those responsible for correcting security deficiencies identified during the Security Assessment and Authorization (SA&A) process.

140.1.4.7 Information System Security Officer (ISSO). The ISSOs are responsible for ensuring that the appropriate security posture is maintained for TIGTA's information systems under their purview. The ISSOs ensure that all applicable security controls are implemented and maintained, and that procedures to implement security controls are documented. The ISSOs ensure the system is properly monitored for vulnerabilities or weaknesses and they are addressed/remediated accordingly. They facilitate timely completion and reporting of required continuous monitoring activities. The ISSOs coordinate with the System Owner to ensure changes to the system are controlled in accordance with applicable change management policies, and security impacts of proposed changes are evaluated by or reported to officials responsible for change

control. The ISSOs also communicate existing or potential security issues to the System Owner.

140.1.4.8 System Administrator. System administrators are responsible for implementing all controls in this policy that are applicable to the system, application, or device to which they are assigned. System administrators work with the CISO, IT A&A Team, ISSOs, and other IT staff in the implementation of security responsibilities and maintenance of security requirements. System administrators create system-level POA&Ms in response to any security vulnerabilities discovered, ensure corrective actions are implemented, and provide evidence that weaknesses have been successfully remediated.

140.1.4.9 Service Desk Personnel. The Service Desk Personnel staff responds to user requests for support. If the staff cannot resolve the request, the staff is responsible for referring the user to the appropriate individual or group for a resolution. For security incidents, the staff should forward the incident to the A&A Team.

140.1.4.10 Managers and Supervisors. Managers and supervisors ensure that subordinates comply with this security policy and pursue appropriate action for noncompliance. They must notify system owners to revoke access privileges in a timely manner when a user under his/her supervision or oversight no longer requires access privileges, requires a change in access privileges, or fails to comply with stated policies or procedures.

140.1.4.11 Contracting Officer's Representatives (COR). The CORs are responsible for working with the CISO to determine whether contractors require IT system access in order to accomplish tasks. The CORs in conjunction with the CISO review and authorize access privileges for contractors and review user security agreements on at least an annual basis to verify the continuing need for access, the appropriate level of privileges, and the accuracy of information contained in the agreement (*e.g.*, systems authorized for access and type). The COR works with the CISO to ensure IT security requirements are fully addressed in IT procurements.

140.1.4.12 End Users. TIGTA end users are responsible for adhering to applicable end user security controls in this policy, such as appropriate use of information to which they have access and devices to which they are assigned. It is also the responsibility of the end user to be aware of the security of TIGTA's IT systems and ensure proper handling of any sensitive information within the system. End users are responsible for completing IT security awareness training in accordance with established timeframes. End users must report any suspected security incidents in a timely manner, and cooperate in the investigation of such incidents.

140.1.5 Policy.
This policy provides TIGTA with a common structure for identifying and managing cybersecurity risks across the enterprise and provides information system personnel

with guidance for assessing the maturity of controls to address those risks. This policy also provides TIGTA with a meaningful independent assessment of the effectiveness of its information security programs.

TIGTA protects its IT information systems by implementing the security controls, creating POA&Ms for remediation, or accepting the risk of the control failure contained in the documents below:

- NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations;
- Treasury Directive Publication (T DP) 85-01 Treasury Information Technology Security Program;
- TIGTA defined Information Security Policies and Exhibits in Chapter (500)-140.

The NIST SP 800-53 is the primary document to be used to determine applicable security controls for TIGTA IT systems. In order to make a determination on a control's implementation criteria, TIGTA also needs to use Treasury's Information security policies and TIGTA's Bureau-defined values, providing additional guidance and implementation criteria that augment the NIST 800-53 and TD P 85-01 controls. Any questions around the FISMA security controls should be e-mailed to TIGTA's CISO at *TIGTAITCSIRC@tigta.treas.gov.

140.1.6 Cognizant Authority.
The TIGTA Cybersecurity Team is responsible for the maintenance of this policy. This policy must be reviewed at least every three years or if there is a significant change.

DATE: April 1, 2020

CHAPTER 500 – INFORMATION TECHNOLOGY

140.2 Acceptable Use Policy

140.2.1 Overview.
This Acceptable Use Policy is intended to outline expected behavior in regards to the use of Government information technology (IT) resources and to delineate between authorized and unauthorized operating practices. This Acceptable Use Policy also provides an overview of IT system security policies mandated by TIGTA. All Government IT resources, including but not limited to, hardware, software, storage media, and computer and network accounts, provided by TIGTA are the property of TIGTA. They are to be used for business purposes in serving the interests of the Government and TIGTA customers in the course of normal operations. Use of Government IT resources for purposes other than those identified within this policy are strictly prohibited and could negate the security of TIGTA IT systems. Effective security is a team effort involving the participation and support of everyone who deals with information and/or information systems. It is the responsibility of everyone to know these guidelines, and to conduct their activities accordingly.

140.2.2 Purpose and Management Commitment.
The purpose of this policy is to outline the acceptable use of TIGTA owned, leased, or otherwise controlled IT resources. This policy is intended to supplement the TIGTA Operations Manual Chapter (500)-140, Information Security by defining specific provisions for the limited use of Government IT resources and summarizing TIGTA IT system policy and best practices.

This policy represents the commitment of TIGTA to ensuring that system and information integrity policy is appropriately defined and implemented, in order to protect TIGTA systems from intentional or unintentional acts that may negatively impact system security.

140.2.3 Scope.
This policy applies to the use of information, electronic and computing devices, and network resources to conduct TIGTA business. All TIGTA employees, contractors, and vendors are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with TIGTA policies and standards, and local laws and regulation.

This policy applies to employees, contractors, and vendors. This policy applies to all equipment that is owned or leased by TIGTA. This policy covers TIGTA entire operational environment, including telework locations/sites.

140.2.4 Roles and Responsibilities.

Outlined below are the roles and responsibilities associated with the TIGTA information security program and the acceptable use policy.

140.2.4.1 Authorizing Official (AO).
The Authorizing Official (AO) is responsible for the overall management of TIGTA's IT security program. The AO allocates resources to ensure proper identification, implementation, and assessment of common security controls, to include acceptable use policy, on TIGTA IT systems.

140.2.4.2 Chief Information Security Officer (CISO) and Cybersecurity Team.
The Cybersecurity Team, led by the CISO, is responsible for providing oversight and guidance to the Information System Security Officers (ISSO), IT staff, and the TIGTA workforce in complying with TIGTA's IT security program. The Cybersecurity team facilitates the implementation of security controls within TIGTA, on behalf of the CISO, and monitors TIGTA IT systems to ensure compliance. The CISO is also responsible for clarifying security controls.

140.2.4.3 Managers and Supervisors.
Managers and Supervisors must ensure that employees are informed of appropriate uses of Government office equipment and information technology as a part of their introductory training and orientation.

140.2.4.4 End Users.
TIGTA users are accountable to follow the Rules of Behavior and to be responsible for their own personal and professional conduct. The Office of Government Ethics (OGE) Standards of Ethical Conduct states, "employees shall put forth honest effort in the performance of their duties." 5 C.F.R. § 2635.101(b)(5). In addition, the Office of Personnel Management (OPM), Employee Responsibilities and Conduct, states, "[a]n employee shall not engage in criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, or other conduct prejudicial to the Government." 5 C.F.R. § 735.203.

The personal use of Government IT resources requires responsible judgment, supervisory discretion and compliance with applicable laws and regulations. Users are responsible for familiarizing themselves with IT security policies and mandates which are addressed in the Treasury Security Manual, Treasury Directive Publication (TD P) 15-71, TD P 85-01 Treasury Information Technology Security Program, and TIGTA Operations Manual Chapter (500)-140, Information Security.

140.2.5 Definitions.

Employee non-duty time:
Times when the employee is not otherwise expected to be addressing official business. Users may, for example, use Government office equipment during their own off-duty hours such as before or after a workday (subject to local office hours), lunch periods,

authorized breaks, or weekends or holidays as agreed to by the employees and the organization's managers.

Information Technology (IT):
Means any equipment or interconnected system or subsystem of hardware or application software that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data.

Government IT resources:
Includes, but is not limited to: office and telephone equipment, personal computers and laptops (*i.e.*, computer personally assigned to user), related peripheral equipment and application software, library resources, and services (including phone sets, smartphones, and voice mail), facsimile machines, photocopiers, office supplies, Internet connectivity and access to Internet services, and e-mail.

Note: The unauthorized use of franked or official mail (*e.g.* penalty mail, United Postal Service) may result in criminal or civil penalties under 18 U.S.C. § 1030.

Minimal additional expense:
An employee's limited personal use of Government IT resources is confined to (1) those situations where the Government is already providing equipment or services and the employee's use of such equipment or services will not result in any additional expense to the Government or will result in only fair wear and tear, or (2) the use of small amounts of electricity, ink, toner, or paper. Examples of minimal additional expenses include making a few photocopies, using a computer printer to print out a few pages of material, making occasional brief personal phone calls (consistent with Department of Treasury policy and 41 C.F.R. § 101-35), infrequently sending personal e-mail messages, or limited use of the Internet for personal reasons**.**

Personal use:
By an employee, consistent with this policy, is considered an "authorized use" of Government property as the term is used in the Standards of Conduct for Employees of the Executive Branch. 5 C.F.R. § 2635.101(b)(9) and § 2635.704(a).

Privilege:
In the context of this policy, means that TIGTA is extending the opportunity to its employees to use Government property for limited personal use in an effort to create a more supportive work environment. However, this policy does not create the right to use Government office equipment for non-Government purposes (other than personal use consistent with this policy). Nor does the privilege extend to modifying the equipment used, including loading personal software, copying existing software, or making configuration changes. Specific exceptions may be necessary to accommodate staff members with a valid need. Requests for such exceptions must be directed to the employee's first level supervisor.

File Sharing Technology (also known as Peer-to-Peer (P2P)):
Generally refers to any software or system allowing individual users of the Internet to connect to each other and trade computer files. These systems are usually highly decentralized and are designed to facilitate connections between persons who are looking for certain types of files. While there are many appropriate uses of this technology, a number of studies show the vast majority of files traded on P2P networks are copyrighted music files and pornography. Data also suggests P2P is a common avenue for the spread of computer viruses within IT systems, and has been known to dominate a disproportionate segment of an organization's available bandwidth.

140.2.6 Policy.

140.2.6.1 Specific Provisions on the Limited Personal Use of Government Information Technology Resources.
TIGTA employees are granted the privilege to use Government IT resources for non-Government purposes when such personal use meets the following criteria:

a. incurs minimal additional expense and network time to the Government;
b. occurs during non-duty time for reasonable duration and frequency;
c. does not adversely affect the performance of official duties or interfere with the mission or operation of the Agency; and
d. does not violate the Government OGE Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. Part 2635, the Supplemental Standards of Ethical Conduct for Employees of the Treasury Department, 5 C.F.R. Part 3101, the Department of the Treasury Employee Rules of Conduct, 31 C.F.R. Part 0, the TIGTA Operations Manual Chapter (700)-30, Ethics, and the TIGTA IT Rules of Behavior.

140.2.6.2 Inappropriate/Unauthorized Uses.
When using Government IT resources for non-Government purposes, users are not authorized to:

a. create, copy, transmit, or retransmit greeting cards, video, sound or other large file attachments that can degrade the performance of the entire network;
b. utilize "Push" technology on the Internet and other continuous data streams that can also degrade the performance of the entire network. "Push" technology refers to the data distribution method in which data is automatically delivered to a computer or mobile device in real time or at periodic intervals;
c. access pornography or hacker sites;
   Note: This policy statement does not apply to any users working in an official capacity that may require access to certain sites.
d. use Government systems as a staging ground or platform to gain unauthorized access to other systems;

e. use Government IT resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation;
f. create, download, view, store, copy, or transmit sexually explicit or sexually oriented materials;
g. create, download, view, store, copy, or transmit materials related to any gambling (legal and illegal), illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited;
h. download, copy, and/or play computer video games;
i. use Government IT resources for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (*e.g.*, consulting for pay, sales or administration of business transactions, sale of goods or services), including using Government IT resources to assist relatives, friends, or other persons in such activities (*e.g.*, employees may not operate or participate in the operation of a business with the use of TIGTA's IT resources);
j. engage in any prohibited outside fund-raising activity, endorse any product or service, participate in any lobbying activity, or engage in any prohibited partisan political activity;
k. post non-public Government information to external news groups, bulletin boards, social media (*e.g.* Facebook, Twitter) or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate agency approval has been obtained or the use is not at odds with the agency's mission or positions;
l. acquire, use, reproduce, transmit, or distribute any controlled information, including computer software and data, that includes privacy information, copyrighted, trademarked, or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data;
m. download files, for example music or other inappropriate material, for the purpose of forwarding them to another individual. This activity, also known as "file sharing," is considered outside the scope of limited personal use. Furthermore, the use of file sharing technology creates a substantial computer security risk in that it may facilitate the spread of computer viruses;
   Note: TNET provides web filtering software to monitor and track user browser activity in real-time on TIGTA IT systems. Should a TIGTA employee have a valid business need for accessing a particular web site in support of an investigative case or audit, the employee may request access by submitting a bypass request form. Users should contact the TIGTA Service Desk for instructions on how to request access.
n. process or store classified information on an unclassified system;
o. extract information from IRS or other Government entities, and their computer systems (*e.g.*, IDRS, TECS, *etc.*) unless needed for business purposes;
p. reconfigure any TIGTA approved security control, thereby ensuring that mandated security requirements are not inadvertently disabled or modified;

q. store or record unencrypted passwords; and
r. transmit unencrypted sensitive information (*e.g.* passwords, social security number, credit card number, or passport number, *etc.*).

140.2.6.3 Malicious Software.
All employees must remain alert to malicious software often transmitted via e-mail and digital media. Loading and/or executing files or software on an individual workstation may result in damage to Government computers or compromise the security of sensitive Government records. It is therefore imperative that employees exercise appropriate caution in their electronic communications and when loading and/or executing files or software. For more information, refer to TIGTA Operations Manual (500)-140.1 Security Controls for further details on System and Information Integrity, and Media Protection.

140.2.6.3.1 Lab-Based Computers.

a. users must not perform any activities intended to create and/or distribute malicious programs into TIGTA's networks (*e.g.*, viruses, worms, Trojan horses, e-mail bombs, *etc.*) on TIGTA lab-based computers;
b. if lab-testing conflicts with anti-virus software, the user must run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, the user must enable the anti-virus software. When the anti-virus software is disabled, no applications should be running which could transfer a virus, *e.g.*, e-mail or file sharing; and
c. no TIGTA sensitive data should be added to any lab environment without CISO and CIO's approval.

140.2.6.4 E-mail.

140.2.6.4.1 Government E-mail Accounts.

a. users are responsible for maintaining the security of their Government e-mail account and to take precautions to prevent unauthorized access to their mailbox;
b. users must not open any files or macros attached to an unsolicited e-mail. Unsolicited e-mail is defined as any e-mail message received that was mailed from an unknown, suspicious, or untrustworthy source or via a mass mailing list to which the recipient did not subscribe. These messages can include pornographic topics, hoax messages, chain e-mail, spam messages and advertisement messages;
c. suspicious e-mails must be reported by clicking the "Report Phishing" button in the Outlook ribbon;
d. users must not create, copy, transmit, or retransmit of chain letters (a message directing the recipient to forward it to multiple others, typically promising rewards for compliance) or other unauthorized mass mailings regardless of the subject matter;
e. users must delete spam and other junk e-mail without forwarding it;
f. users must not click on or follow any hyperlinks or URLs included in an unsolicited e-mail message;

g. users must not automatically forward e-mail messages to non-Treasury accounts; and
h. TIGTA users must encrypt sensitive information sent via e-mail if the recipient is external to TIGTA.
   Note: Users, who suspect an incident has occurred on any TIGTA information system, are responsible for reporting incidents within an hour, and must immediately refer to SOP-09.22 Incident Response Plan for procedures on how the potential incident should be handled.

Note: TIGTA emails are retained that will be archived and maintained for predetermined time periods in support of Freedom of Information Act (FOIA) or other legal/management purposes.

140.2.6.4.2 E-mail Privacy.
E-mail is a TIGTA asset and a critical component of the communication system. The e-mail system is provided by TIGTA for users to facilitate the performance of their work and the contents are the property of TIGTA. TIGTA management reserves the right to retrieve and view the contents for legitimate reasons, such as to find lost messages, to comply with investigations or legal requests, or to recover from system failure. TIGTA may also use, as it deems appropriate, e-mail content filtering software to implement security policies to detect, block or quarantine inappropriate or threatening incoming Internet e-mails and attachments. As necessary, incoming and outgoing Internet e-mail may be retrieved as part of this policy. TIGTA users should be aware that a copy of every message sent through the TIGTA e-mail system, even if deleted immediately, is archived and retrieved to meet legal requirements.

140.2.6.4.3 Personal E-mail Accounts.

a. TIGTA users must not use non-TIGTA e-mail accounts (*e.g.*, personal e-mail service provider, Hotmail, Yahoo, Gmail) for conducting official duties. Treasury/bureau internal e-mail systems provide sufficient safeguards to allow for the transmission of Sensitive But Unclassified (SBU) information. Refer to Treasury IT Security Program, TD P 85-01 and Treasury Security Manual, TD P 15-71 for additional information. Users with a defined need must submit a request in writing to obtain a waiver from the Chief Information Officer (CIO);
b. personal e-mail service providers' client software must not be installed on TIGTA workstations; and
c. access to personal e-mail accounts from Government IT resources must meet the conditions set forth in Personal Use of Government Information Technology Resources, Treasury Directive (TD) 87-04 and must meet the requirements for limited use.

140.2.6.5 Virtual Private Networks (VPN).

a. users, other than system administrators performing official duties, must not reconfigure any TIGTA-approved VPN technology, thereby ensuring that mandated security requirements are not inadvertently disabled or modified;
b. the use of TIGTA devices are only authorized for TIGTA users to perform official duties. TIGTA laptops must connect to TIGTA VPN or TIGTA's physical network. TIGTA laptops must not be used or connect to any individual's home network to access the internet; and
c. remote access is only permitted through TIGTA-approved remote access technologies, including both hardware and software. TIGTA users must not install or otherwise make available any remote access technology on any TIGTA hardware that is attached to the TIGTA network. If unauthorized remote access instances are discovered, they must be immediately disabled.

140.2.6.6 Encryption.

a. users must encrypt all sensitive data stored on mobile computers/devices in accordance with the TIGTA Operations Manual (500)-140.1 Security Controls, Media Protection (MP) requirement;
b. users must not reconfigure any TIGTA approved encryption system, thereby ensuring that mandated security requirements are not inadvertently disabled or modified;
c. electronically transmitting sensitive material must be in accordance with TIGTA Operations Manual (500)-140.4, Sensitive Information Protection Policy. Classified material must never be transmitted on the TIGTA's unclassified e-mail system; and
d. users must use secure messaging when transmitting sensitive information via the TIGTA e-mail system. Refer to Hardware/Software FAQ for more information on secure message procedures.

140.2.6.7 Workstations.

a. all laptop computers, hardware, or software are assigned to users on an individual basis. Users must take every reasonable precaution to protect such resources from loss or damage in accordance with TIGTA Operations Manual (600)-100.2, Personnel Property Management Program – Policy, and TIGTA Operations Manual (500)-140.4, Sensitive Information Protection Policy;
b. users must not change any security settings on their workstation;
c. users must never leave their workstations unattended and unprotected without locking their workstations. For more information, refer to the TIGTA Operations Manual (500)-140.1 Security Controls, Access Control (AC) requirement;
d. users must not install personal equipment (*e.g.* wireless keyboard), and unauthorized software on TIGTA workstations without the written prior approval of the Change Management Board (CMB). However Government procured or personally owned monitors with no storage media (e.g. smart TVs or smart monitors capable of processing, storing, or transmitting data) attached, or wired/wireless mouse are not require approval by the CMB; and

e. users must not clear the application, security or system event logs.

140.2.6.8 Users with Privileged User Accounts.
Privileged user accounts include any user account that is granted elevated access privileges on IT system resources. For this purpose, privileged user accounts are those that allow for the installation or configuration of software on any Treasury asset. The use of privileged user accounts is only approved for conducting official IT system administration duties.

a. users assigned privileged user accounts must not use their privileged accounts for Internet browsing or other Internet connections outside of the local protected boundary unless authorized in writing by the TIGTA CIO or a CIO-designated alternate;
b. users with privileged user accounts must not use those accounts to initiate a remote access session to TIGTA network resources via VPN;
c. users with privileged user accounts must not use their privileged accounts to access their TIGTA e-mail mailbox. All users must use their normal user (non-privileged) account to access their TIGTA e-mail mailbox to send and receive e-mail;
d. due diligence must be taken by user and/or manager to inform systems maintenance personnel when privileged user accounts are no longer needed. This facilitates the removal of unnecessary access at the earliest possible time; and
e. users with accounts with privileged access must use those accounts only when needed to perform their duties. Normal daily activities must be conducted using non-privileged accounts.

140.2.6.9 Proper Representation.
It is the responsibility of employees to ensure that they are not giving the false impression that they are acting in an official capacity when they are using Government IT resources for non-Government purposes. If there is an expectation that such a personal use could be interpreted to represent an agency, then an adequate disclaimer must be used. One acceptable disclaimer is –

> The content of this message is mine personally and does not reflect the position of the U.S. Government, the Department of the Treasury, or the Treasury Inspector General for Tax Administration.

The OGE Standards of Ethical Conduct states that, "…an employee shall not use or permit the use of his Government position or title or any authority associated with his public office in a manner that could reasonably be construed to imply that his agency or the Government sanctions or endorses his personal activities." 5 C.F.R. § 2635.702(b). In addition, users should review 5 C.F.R. § 2635.704 concerning the use of Government property, 5 C.F.R. § 2635.705, Use of Official Time, and 31 C.F.R. § 0.213 concerning general conduct.

140.2.6.10 Privacy Expectations.
Employees do not have a right, nor should they have any reasonable expectation, of privacy while using any Government IT resources at anytime, including accessing the Internet or using e-mail. To the extent that employees wish that their private activities remain private, they should avoid using Government IT resources such as their TIGTA-issued computer, the Internet access, or e-mail for such activities. By using Government IT resources, employees give their consent to disclosing the contents of any files or information maintained using this equipment. In addition to access by TIGTA officials, data maintained on Government IT resources may be subject to discovery and Freedom of Information Act, 5 U.S.C. § 552, requests. By using Government office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet or using e-mail. Any use of Government telecommunications resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

140.2.7 Cognizant Authority.
The TIGTA IT Cybersecurity Team is responsible for the maintenance of this policy. This policy must be reviewed at least every three years or if there is a significant change.

DATE: April 1, 2020

CHAPTER 500 – INFORMATION TECHNOLOGY

140-3 Breach Notification Policy

140.3.1 Overview.
This Breach Notification Policy establishes a framework within the Treasury Inspector General for Tax Administration (TIGTA) for addressing a data breach while ensuring proper safeguards are in place to protect sensitive information such as Personally Identifiable Information (PII). This policy also addresses incident response regarding PII, risk categorization and analysis, and safeguarding against breaches of PII.

140.3.2 Scope.
This Breach Notification Policy applies to all sensitive data maintained and controlled by TIGTA, including external organizations on behalf of TIGTA. This policy applies to information and information systems in any format (*e.g.*, paper, electronic) and does not distinguish between suspected and confirmed breaches.

140.3.3 Definitions.
OMB Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information defines the PII as "information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, *etc*., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, *etc*.". Treasury Directive (TD) 25-08, Safeguarding Against and Responding to the Breach of Personally Identifiable Information defines a breach as: "the suspected or actual loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII whether in physical or electronic form".

140.3.4 Background.
In response to OMB Memorandum M-07-16, TIGTA developed this Breach Notification Policy to outline protective measures that must be followed by TIGTA personnel, contractors, and vendors if there is a breach within TIGTA.

140.3.5 Roles and Responsibilities.
Core Management Group (CMG). TIGTA's CMG will be convened by the Chief Information Security Officer (CISO) upon the identification of a potential breach of PII. The CMG should include the manager of the program experiencing the breach, Chief Information Officer, Office of Chief Counsel, Office of Investigations, and the Office of Mission Support, which includes the Communications and Finance & Procurement Services functions. The CISO is a non-voting member for the convent. Guidance for the group's composition is contained in OMB M-07-16. The CMG will initially evaluate the situation to help guide any breach notification response.

In certain circumstances, the CMG will not be convened on an initial breach determination. This will only occur if the investigation of an incident involving PII reveals there is no or little risk of harm to TIGTA from the potential breach of PII. The CISO must ensure there are procedures in place to:

- identify the specific types of incidents where the CMG will not be convened on an initial breach determination;
- ensure there are two separate reviews of the incident and concurrent independent recommendations to not convene the CMG; and
- create a process that allows any CMG member to request the group be convened if they think any potential breach was closed inappropriately.

140.3.6 Policy.

140.3.6.1 Security Categorization. TIGTA must confirm that the security category of the information system has been determined and documented in the system security plan and review the FIPS 199 security categorization described in the system security plan to determine if the assigned impact values with respect to the potential loss of confidentiality, integrity, and availability are consistent with agency's actual mission requirements. The determination of the potential impact of loss of information is made during an information system's certification and accreditation process.

- low: the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets or individuals;
- moderate: the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets or individuals;
- high: the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.

The impact levels will help determine when and how notification should be provided. Where there is a range of risk levels attributed to the factors, the decision to provide notification should give greater weight to the likelihood the information is accessible and usable and whether the breach may lead to harm (*e.g.*, identify theft).

140.3.6.2 External Breach Notification. The CMG will use the procedures contained in TIGTA's Breach Notification Procedure, SOP-09.23 for making a breach notification determination and response. All TIGTA users must follow TIGTA's Breach Notification Procedure, SOP-09.23, in the event of an information or information system breach.

TIGTA's Office of Chief Counsel must be notified and consulted in the event of a breach of PII and before any breach notification occurs to determine if the notification is authorized.

140.3.6.3 Risk Assessment. Whether breach notification is required must be based upon the likely harm caused by the breach and by assessing the level of risk. Likely harm should be determined by considering five (5) factors:

- the nature of the data elements breached;
- the number of individuals affected;
- the likelihood the PII will be or has been compromised – made accessible to and usable by unauthorized persons;
- the likelihood the breach may lead to harm; and,
- the ability of the agency to mitigate the risk of harm.

If a loss of personal information poses a high risk of identity theft, exposure, and harm, as determined by CMG, notification will be made to the affected individuals, contingent upon Chief Counsel's review and authorization.

140.3.6.4 Incident Reporting. The OMB memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, requires agencies to report all incidents involving PII to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovering the incident. Pursuant to the TD 25-08, and Treasury Directive Publication (TD P) 85-01, Treasury Information Technology Security Program, TIGTA will continue to report the occurrence of losses of PII in electronic or physical form to the Treasury Computer Security Incident Response Center/Global Security Operations Center (TCSIRC/GSOC) in accordance with standing requirements.

TIGTA shall report breaches or incidents, whether confirmed or suspected, to the GSOC as quickly as possible after discovery and in no more than one business day. TIGTA will not wait for absolute confirmation of a breach or incident before reporting. In addition, TIGTA must update incident and breach reports tracked by GSOC according to the parameters in the Departmental Incident Response Plan.

For any incident involving PII, TIGTA must include the existing and new requirements specified in the OMB M-07-16, Attachment 2: Incident Reporting and Handling Requirements. TIGTA must follow the specified FISMA requirements, and apply the incident handing and response mechanisms specified in TIGTA's Incident Response policy and procedures. TIGTA must report all PII incidents through GSOC to US-CERT within one hour of discovery/detection.

140.3.6.5 Privacy and Security Awareness Training. All TIGTA users must receive the annual Security Awareness Training and Privacy Awareness Training. TIGTA requires

that all users be informed and trained regarding their respective responsibilities relative to safeguarding PII and the consequences and accountability for violation of these responsibilities. TIGTA must educate its employees and other authorized entities with access to PII (*e.g.*, through a data sharing agreement) regarding the rules to safeguard information and information systems, the breach notification process in the event of a breach, and the potential consequences of the breach.

140.3.7 Cognizant Authority.
The TIGTA Cybersecurity Team is responsible for the maintenance of this policy. This policy must be reviewed at least every three years or if there is a significant change.

DATE: July 1, 2020

CHAPTER 500 – INFORMATION TECHNOLOGY

140-4 Sensitive Information Protection Policy

140.4.1 Overview. This Sensitive Information Protection Policy applies to all functions of the Treasury Inspector General for Tax Administration (TIGTA) and establishes TIGTA information security guidelines for the proper classification and protection of information that should not be disclosed to non-TIGTA employees or outside of TIGTA without proper authorization.

140.4.2 Scope. The procedures for safeguarding information contained in this policy apply to information that is either stored or shared via any means and designated as Sensitive but Unclassified (SBU) information, including Personally Identifiable Information (PII). This includes electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All TIGTA employees, contractors, and vendors (users) are personally responsible for providing proper protection to SBU information under their custody and control.

140.4.3 Information Classification.

140.4.3.1 Classification Categories. Information is categorized into the following classifications: Classified, SBU, and Public. Although, to date, all information originating with TIGTA and processed on TIGTA systems has been designated as SBU, the applicable Classification Authority (CA) is responsible for the classification/ declassification and proper handling and control of classified information and must follow the guidance contained in Treasury Order (TO) 105-19, Executive Order (EO) 12958, and Chapter III, Section 24 of Treasury Directive (TD) P 15 -71. Since the procedures for safeguarding information contained in this policy apply only to information designated as SBU, the CA should contact the TIGTA Chief Information Security Officer (CISO) regarding classified information.

Currently TIGTA is not authorized to electronically store any classified information. If users suspect they are electronically storing or manipulating classified information on TIGTA systems, they should report this to their manager and the CISO immediately.

140.4.3.2 Sensitive but Unclassified (SBU) Information. Under the current designation, SBU, as defined by the Computer Security Act of 1987, is any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act of 1974, 5 U.S.C. § 552a, but not specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy. As required by TD P 15-71, SBU shall be the primary term used to mark sensitive but unclassified information

originating within TIGTA. The SBU marking shall identify information, the release of which may adversely impact economic, industrial, or international financial institutions; or compromise unclassified programs or TIGTA essential operations or critical infrastructures. Previous designations used to label sensitive information (*e.g.*, OFFICIAL USE ONLY (OUO), LIMITED OFFICIAL USE, and LAW ENFORCEMENT SENSITIVE (LES)) are to be discontinued unless authorized. See TD P 15-71, Chapter III, Section 24.

TIGTA users must safeguard PII in the same manner as all other SBU information processed on TIGTA systems. PII is any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, *etc*. alone or, when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, *etc*. PII that is processed, stored or transmitted on TIGTA systems is designated as SBU.

SBU information is to be safeguarded commensurate with the risk and magnitude of the harm that would result from their being lost, misused, accessed without authorization, or modified. SBU materials are accessible only for official purposes and as the law permits. Information that is to be protected very closely, includes but is not limited to, developmental programs, law enforcement issues, taxpayer information (including tax return information), attorney-client privileged material, attorney work product, grand jury material, and other privileged information integral to the operations of TIGTA and the functions it performs.

140.4.3.3 Public. TIGTA Public is any unclassified TIGTA information that has been declared public knowledge by those with the authority to do so, and can be freely given to anyone without any possible damage to TIGTA.

140.4.3.4 Declassification. It is the Classification Authority's responsibility to authorize a change in classification status of information. Declassification of documents must be conducted in accordance with 31 C.F.R. Part 2, and Chapter III of TD P 15-71.

140.4.4 Document Markings. Every document designated as TIGTA SBU should be marked to show the level of sensitivity of information it contains. No markings are required for TIGTA Public materials since disclosure of this information will not prove harmful to TIGTA.

Markings should be applied at the time documents are drafted to promote proper protection of the information. These markings must be conspicuous enough to alert anyone handling the documents that they contain SBU information.

The SBU markings must follow TD P 15-71 Chapter III, Section 24, Sensitive But Unclassified Information.

The lack of SBU markings; however, does not relieve the holder from safeguarding responsibilities. Unmarked SBU information already in records storage does not need to be removed, marked, and restored. However, when individual items are temporarily removed from storage that have no markings (and are subsequently deemed to be SBU) they should be appropriately marked to reflect the correct status as SBU before being re-filed.

Items containing SBU information should be:

a. Prominently marked at the top/bottom of the front/back cover and each individual page with the marking "SENSITIVE BUT UNCLASSIFIED" or "SBU." Information system prompts may be adjusted to incorporate SBU markings in headers and footers.

c. Controlling, decontrolling or originator information markings are not required.

d. When sent outside TIGTA, SBU information documents should include a statement alerting the recipient in a transmittal letter or directly on the document containing SBU information, for example: *This document belongs to the Treasury Inspector General for Tax Administration (TIGTA). It may not be released without the express permission of TIGTA. Refer requests and inquiries for the document to: (insert name, bureau address and contact number(s)).*

140.4.5 Control Measures. Each TIGTA function is responsible for establishing a system of control measures for their units, to ensure that access to TIGTA information is limited to authorized persons. The control measures must be appropriate to the environment in which the access occurs and relevant to the information. The system must include technical, physical, and personnel control measures. Administrative control measures, which may include records of internal distribution, access, generation, inventory, reproduction, and disposition, must be required when technical, physical, and personnel control measures are insufficient to deter and detect access by unauthorized persons.

140.4.6 Access Clearance for TIGTA SBU. TIGTA Personnel Security must ensure that all TIGTA employees, contractors, and vendors complete all appropriate clearance forms in order to access TIGTA SBU.

140.4.7 Safeguarding.

140.4.7.1 General Policy. All SBU information in TIGTA's custody and/or control must be appropriately safeguarded regardless of location (*e.g.*, workspace, during transport, *etc.*). The SBU information must be protected irrespective of how it is maintained, whether accessible from a TIGTA computer, paper-based, or stored on media (*e.g.*, disk, tape, optical disc, thumb or Universal Serial Bus (USB) drive, or other storage/recording media). Classified information must not – under any circumstances - be processed on TIGTA systems. Classified information (*e.g.*, Secret or Top-Secret) is

expressly prohibited from being stored on TIGTA computer equipment (*e.g.*, laptop, file servers, network storage, *etc.*) or transmitted over the TIGTA network.

TIGTA users must adhere to the Information Systems Security Rules of Behavior. TIGTA users are also responsible for being familiar with TIGTA Information Technology Security Policies, which provide guidance on information classification and sensitivity and the appropriate use of information technology resources in accessing and transmitting SBU information. The failure to safeguard national security information constitutes a security violation. The failure to properly safeguard SBU information may be considered a procedural deficiency. Security violations are to be handled in accordance with TD P 15-71, Chapter III, Section 19, Handling Security Infractions, Investigating and Adjudicating Reported Security Violations.

Any TIGTA user who does not understand how information should be safeguarded should verify Treasury handling policy from TD P 15-71 Chapter III Sensitive But Unclassified Information. If guidance cannot be readily obtained, the user should secure the information until a complete understanding of his/her responsibilities in protecting and handling the information is obtained.

140.4.7.2 Basic Handling Guidelines for SBU Information. In addition to TIGTA Information Technology Security Policies, the following guidelines must be followed:

- SBU information must only be processed on TIGTA-owned devices;
- TIGTA users must not share or discuss SBU information, security procedures, (such as alarm systems, *etc.*), with unauthorized staff or other individuals who have no business need-to-know;
- SBU information must not be stored in voice mails;
- TIGTA users must never provide copies of written correspondence, directories, or manuals to people outside of TIGTA unless otherwise authorized to do so by management* (this may require multiple levels of approval).

* Resources available on TIGTA's Freedom of Information Act Library, to include the Operations Manual, may be disseminated to those outside TIGTA.

140.4.7.3 Storage.

140.4.7.3.1 TIGTA Applications. SBU information maintained within TIGTA business applications (*e.g.*, TeamMate, Criminal Results Management System, Data Center Warehouse, *etc.*) must not be extracted from these applications unless needed for business purposes. TIGTA users who download SBU information are responsible for safeguarding the information in accordance with Office of Management (OMB) Memorandum 06-16 Protection of Sensitive Agency Information, OMB Memorandum 17-12 Preparing for and Responding to a Breach of Personally Identifiable Information, Treasury, and TIGTA policy requirements.

140.4.7.3.2 IRS and Government Applications. TIGTA users who obtain information from the Internal Revenue Service (IRS) or other government entities and their computer systems (*e.g.*, Integrated Data Retrieval System, TECS, *etc.*) are responsible for safeguarding the information in accordance with OMB Memorandum 06-16 Protection of Sensitive Agency Information, Treasury, and TIGTA policy requirements and also in accordance with its classification (regardless of which agency classifies the information). Information must not be extracted from these applications unless needed for business purposes.

140.4.7.3.3 Network Storage. TIGTA users are encouraged to store information on their personal drive (Z: drive) or another appropriate network location (*e.g.*, group folder). The Office of Information Technology (OIT) performs regular backups on network storage and can recover most lost information from backups, if needed. Using network storage reduces the risk of information being lost or stolen versus storing data on a laptop computer or removable media.

Note: Classified information may not be stored or transmitted on any TIGTA computer equipment (*e.g.*, Z: drive or other network storage, laptop, or on thumb or USB drives).

140.4.7.3.4 Laptop Computers. TIGTA users must adhere to the following guidelines when storing information on laptop computers:

- SBU information must only be saved to the hard drive (*i.e.,* D: drive) of a laptop computer when required to conduct necessary business.

TIGTA users desiring backup of information should store such information, without encryption, on their Z: drive or another appropriate network location. TIGTA OIT does not backup laptop hard drives and cannot guarantee recovery of any information saved to the laptop hard drive.

140.4.8 SBU Protection Procedures for Telecommuters. Telecommuting poses additional risks to the protection and safeguarding of SBU information. The best practice is to limit the amount of SBU information maintained at the alternate worksite. Whenever possible, access data from the application, web site or system that stores and maintains the SBU information, rather than downloading/encrypting the information or printing it.

When maintaining information and records at an alternate worksite, TIGTA users are responsible for safeguarding the information from third parties who may enter or have access to the alternate worksite. The following rules must be observed by TIGTA users when telecommuting:

- Telecommuters must lock the laptop computer screen before leaving it unattended;
- Telecommuters must use authorized storage facilities for storing TIGTA materials (*e.g.*, locked container such as a file cabinet, desk with a locked drawer). In

addition, TIGTA users are encouraged to secure media and the laptop computer (powered off) in a locked container (*e.g.*, cabinet or brief case) when not in use;
- Telecommuters must be careful not to leave TIGTA material unattended or within view of third parties (including family members not authorized to view TIGTA information);
- Telecommuters must be careful to conceal SBU information when approached by visitors; and
- Telecommuters must follow specific procedures for the disposal, transfer, or distribution of storage media that contains or have contained TIGTA materials.

Refer to TIGTA Telecommuting Resources intranet page and Chapter (200)-80.10 Security, for additional guidance in telecommuting security.

140.4.9 Transmission and Transportation.

140.4.9.1 Shipping SBU Information. If a TIGTA user has a need to ship SBU information, media, and/or computer equipment, appropriate precautions must be taken. The method for shipping SBU information and equipment must provide for a chain-of-custody from the point of acceptance by a carrier to the point the package is delivered to its intended recipient. Registered U.S. Mail, Certified U.S. Mail and/or an equivalent commercial service are appropriate methods of shipping that provide chain-of-custody.

140.4.9.2 Additional Restrictions for Shipping SBU Information. SBU information must be transmitted within and between the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and United States territories or possessions by one of the means established for higher classifications, or by the United States Postal Service registered mail. Refer to TD P 15-71, Chapter III, Section 24 for more detail. Outside these areas, SBU information must be transmitted only as is authorized for higher classifications and a receipt is mandatory.

140.4.9.3 Escort or Hand-Carrying of SBU Material. The escorting or hand-carrying of SBU material between Treasury Bureaus and/or Federal agencies or within the same Bureau requires escort or handling personnel to have the same level of authorization clearance as the material in their charge.

140.4.9.4 Information Transmitted via E-mail. TIGTA provides a secure messaging system for encryption of e-mail messages and attachments. Secure messaging requires enrollment and TIGTA users are responsible for ensuring they have enrolled. For IRS users to view TIGTA's secured messages, the IRS users must also be enrolled in secure messaging; the IRS must enroll its own users. Any TIGTA user who needs to enroll in secure messaging, or needs assistance in using secure messaging, should contact the TIGTA OIT Service Desk.

- Secure messaging must be used when e-mailing SBU information to IRS users;

- When e-mailing SBU information to another TIGTA user, use of Secure Messaging is strongly recommended whenever practical and it does not impede TIGTA business practices (*e.g.*, use of shared e-mail boxes and reading e-mail messages from a smartphone);
- When e-mailing SBU information to other governmental agencies which are not enrolled in secure messaging, alternative encryption methods must be used. When using alternative encryption methods that utilize passwords, strong passwords must be used in accordance with Chapter (500)-140.1, of the Security Controls; and
- TIGTA users are prohibited from sending unencrypted SBU information to non-TIGTA e-mail accounts, unless expressly authorized to do so by the TIGTA Chief Information Officer (CIO) and CISO; and
- SBU information must never be sent to personal email accounts (e.g. gmail, hotmail, yahoo, etc) at any time.

140.4.9.5 Information Transmitted via Fax. When faxing SBU information, TIGTA users must monitor transmittals closely to ensure that information is not inappropriately transmitted or received. For example: alert the intended recipient of the fax via telephone that he/she should standby to receive the transmission.

140.4.9.6 Traveling with Information, Records and Computer Equipment.

- When traveling, TIGTA users must maintain personal control of SBU information and records at all times; and
- TIGTA users must not check luggage containing SBU information, records and/or computer equipment while traveling. Refer to Chapter (500)-140.1, Security Controls, for more information.

140.4.10 Emergency Planning. Plans must be developed for the protection, removal, or destruction of SBU material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of its compromise. The level of detail and amount of testing and rehearsal of these plans should be determined by an assessment of the risk of hostile action, natural disaster, or terrorist activity that might place the information in jeopardy.

When preparing emergency plans, consideration should be given to:

- Reduction of the amount of SBU material on hand;
- Storage of less frequently used SBU material at more secure locations; and
- Transfer of as much retained SBU information to microforms or to magnetic media whenever possible to reduce bulk and to aid recreation in an emergency.

140.4.11 Incident Reporting. Any loss or theft of information and/or equipment must be reported immediately after becoming aware of the loss or theft to the TIGTA user's manager, the OIT Service Desk, TIGTA's Computer Security Incident Response

Capability (CSIRC),, and the Special Investigations Unit. This includes the loss or theft of removable media (*e.g.*, disk, tape, optical discs, USB thumb or USB drive, or other storage/recording media), paper-based information and records, and computer equipment (*e.g.*, laptop computers, smartphone devices). The loss or theft must be reported irrespective of the fact that the lost or stolen data was encrypted.

OI will make an investigative determination and take appropriate measures to investigate the loss or theft with support from the OIT, as needed. The OIT Service Desk will notify appropriate OIT personnel for operational response including the TIGTA Incident Response Team, which is responsible for reporting incidents to the Treasury Cyber Security Incident Response Center (TCSIRC), the Treasury's Government Security Operations Center (GSOC) and the related entities. For incidents that include loss of any PII and other information protected by Federal statute (*e.g.*, Privacy Act, I.R.C. § 6103) are to be reported to the TCSIRC as close as possible to the time of incident discovery, within 24 hours. Refer to National Institute of Standards and Technology (NIST) SP 800-61 Rev 2, Computer Security Incident Handling Guide.

140.4.12 Destruction. Media containing SBU information must be destroyed in accordance with Department of Treasury Memorandum for the Destruction of Classified and Sensitive Information, and TD P 80-05 Treasury Records and Information Management Manual.

- The SBU information in electronic form (CD/DVD, USB drives, computer tapes, *etc.*) must be destroyed by the use of an approved degausser or other approved means, in accordance with applicable guidance. The SBU information in electronic form must be placed in its own burn bag and kept separate from SBU paper waste. Contact the CISO for further information concerning the destruction of electronic media containing SBU information;
- The SBU information in paper form must be shredded or disposed of in burn bags;
- All Public Information, such as public-use documents, copies of the *Federal Register* or other publications, magazines, newspapers, press releases, scrap paper that need to be disposed of must be placed in trash or GSA/other recycling box, as appropriate. Public Information in paper or electronic form may be discarded with other non-paper waste.

140.4.13 Termination Briefings. TIGTA Managers must ensure that employees who either leave the organization or whose clearance is terminated receive a termination briefing from the Personnel Security Office as part of their checkout process. This briefing must emphasize their continued responsibility to:

- Protect TIGTA information to which they have had access;
- Provide instructions for appropriately transferring or disposing of SBU information in their possession;

- Advise the individuals of the prohibition against retaining material when leaving the organization;
- Provide instructions for reporting any unauthorized attempt to gain access to such information; and
- Remind them of the potential civil and criminal penalties for failure to fulfill their continuing security responsibilities.

Refer to TIGTA Operations Manual (600)-70.3, Employee Exit Clearance Procedures for complete guidance.

140.4.14 Cognizant Authority. The TIGTA Cybersecurity Team is responsible for the maintenance of this policy. This policy must be reviewed at least every three years or if there is a significant change.