INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

August 28, 2017

TIGTA #17-28
MEMORANDUM FOR TIGTA EMPLOYEES (NON-SUPERVISORY)

FROM: Mervin Hyndman
Acting Deputy Inspector General for Mission Support/
Chief Financial Officer

SUBJECT: Mandatory Drug-Free Workplace Training for Employees (Non-Supervisory)

As mandated by Executive Order (EO) 12564, Drug-Free Federal Workplace, all agencies are to provide mandatory training to all employees for awareness of the Drug-Free Workplace Program. Further, agencies are also required to report the number of employees who have completed this training.

To ensure compliance with this EO, the Office of Mission Support's Human Capital & Personnel Security Directorate will continue to provide training for all Treasury Inspector General for Tax Administration (TIGTA) employees. This training will enhance TIGTA employee awareness of the EO and the Governmentwide effort demonstrating that illegal drugs will not be tolerated in the Federal workplace.

Non-supervisory employees are required to complete the *TIGTA Drug-Free Workplace Training for Employees* by **Friday, September 29, 2017**. This training has been assigned to you via the Treasury Learning Management System (TLMS).

If you have any questions about this requirement, please contact TIGTA Drug-Free Workplace mailbox at tigtadfwp@tigta.treas.gov. For TLMS assistance, please contact the TLMS Helpdesk at (304) 480-8000, option 4, or your function's TLMS Administrator.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

August 1, 2017

TIGTA #17-27
MEMORANDUM FOR ALL TIGTA EMPLOYEES

FROM: Mervin Hyndman
Acting Deputy Inspector General for Mission Support/
Chief Financial Officer

SUBJECT: Foreign Travel Reporting Requirements

This memorandum provides interim guidance on foreign travel reporting requirements. The Office of the Director of National Intelligence's Security Executive Agent Directive 3 (SEAD 3), *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position* (Attachment "A") establishes foreign travel reporting requirements for covered individuals who have access to classified information or hold a sensitive position (*i.e.*, those eligible for a national security clearance). SEAD 3 also requires covered individuals to be aware of the risks associated with possible terrorist activities and/or foreign intelligence operations, recognize and avoid personal behaviors and activities that may adversely impact their continued national security eligibility, and report potential security or counterintelligence concerns of other covered individuals. SEAD 3 became effective **June 12, 2017**.

All Treasury Inspector General for Tax Administration (TIGTA) covered individuals are required to report planned foreign travel, both official and unofficial, to TIGTA Personnel Security (PERSEC) Services and receive approval prior to travel. TIGTA PERSEC will notify Treasury's Office of Counterintelligence (OCI) of planned foreign travel of TIGTA employees to ensure the employees are provided with information on any potential threats or risks associated with the foreign location(s) they are planning to visit. OCI may schedule a personal briefing, either in person or by teleconference, with the employee regarding his/her specific foreign travel plans. Under certain circumstances, an employee's unofficial foreign travel may be disapproved and an employee's failure to comply with any disapproval may result in administrative action, including but not limited

to, revocation of national security eligibility.

TIGTA employees that do not occupy a sensitive position (*i.e.*, occupants of non-sensitive public trust positions) are strongly encouraged to follow this reporting procedure when planning foreign travel as the information provided by OCI may prove beneficial when traveling abroad.

If a TIGTA employee experiences a counterintelligence-related incident or encounters circumstances that cause him/her to feel concerned that he/she may be a target of exploitation by foreign personnel or an entity while on foreign travel, the employee should report the matter to OCI immediately via email at ci@treasury.gov or via its 24 hour hotline at 202-622-1348 and to TIGTA's PERSEC Services via email at *TIGTAPersonnelSecurityOffice@tigta.treas.gov.

For additional information on foreign travel requirements and guidance on mitigating risks while traveling overseas, attached is an August 19, 2015 email sent to all Treasury employees on behalf of the Deputy Secretary and the Assistant Secretary for the Office of Intelligence and Analysis (Attachment "B") and a List of TIGTA Sensitive Positions (Attachment "C").

TIGTA's Operations Manual will be updated to incorporate this interim guidance. Should you have any questions or concerns regarding the information provided in this correspondence, please contact Chevalier Goldring, Assistant Director/SO via secure email at Chevalier.Goldring@tigta.treas.gov or via telephone at 202-927-1046.

Attachments:

A - Security Executive Agent Directive 3
B - Security Guidance from Deputy Secretary Raskin and Assistant Secretary Ireland
C - List of TIGTA Sensitive Positions

Attachment "A"

SEAD 3 Reporting Requirements for Per:

Attachment "B"

Security Guidance from Deputy Secretar

Attachment "C"

LIST OF TIGTA SENSITIVE POSITIONS

SECURITY EXECUTIVE AGENT DIRECTIVE 3

REPORTING REQUIREMENTS FOR PERSONNEL WITH ACCESS TO CLASSIFIED INFORMATION OR WHO HOLD A SENSITIVE POSITION

(EFFECTIVE: 12 JUNE 2017)

A. AUTHORITY: The National Security Act of 1947, as amended; Intelligence Reform and Terrorism Prevention Act of 2004, as amended; Executive Order (EO) 10450, *Security Requirements for Government Employment*, as amended; EO 12968, *Access to Classified Information*, as amended; EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*; EO 13549, *Classified National Security Information Program for State, Local, Tribal and Private Sector Entities*; Presidential Decision Directive/NSC-12, *Security Awareness and Reporting of Foreign Contacts*; Performance Accountability Council memorandum, *Assignment of Functions Relating to Coverage of Contractor Employee Fitness in the Federal Investigative Standards*, 6 December 2012; and other applicable provisions of law.

B. PURPOSE: This Security Executive Agent (SecEA) Directive establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position. Nothing in this Directive should be construed to limit the authority of agency heads to impose additional reporting requirements in accordance with their respective authorities under law or regulation.

C. APPLICABILITY: This Directive applies to any executive branch agency or covered individual as defined below.

D. DEFINITIONS: As used in this Directive, the following terms have the meanings set forth below:

1. "Agency": Any "Executive agency" as defined in Section 105 of Title 5, United States Code (U.S.C.), including the "military department," as defined in Section 102 of Title 5, U.S.C., and any other entity within the Executive Branch that comes into possession of classified information or has positions designated as sensitive.

2. "Classified national security information" or "classified information": Information that has been determined pursuant to EO 13526 or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.

3. "Cohabitant": A person with whom the covered individual resides and shares bonds of affection, obligation, or other commitment, as opposed to a person with whom the covered individual resides for reasons of convenience (e.g. a roommate).

4. "Controlled Substance": Any controlled substance as defined in 21 U.S.C. 802.

5. "Covered Individual":

a. A person who performs work for or on behalf of the executive branch who has been granted access to classified information or holds a sensitive position; but does not include the President or (except to the extent otherwise directed by the President) employees of the President under 3 U.S.C. 105 or 107, the Vice President, or (except to the extent otherwise directed by the Vice President) employees of the Vice President under 3 U.S.C. 106 or annual legislative branch appropriations acts.

b. A person who performs work for or on behalf of a state, local, tribal, or private sector entity, as defined in EO 13549, who has been granted access to classified information, but does not include duly elected or appointed governors of a state or territory, or an official who has succeeded to that office under applicable law.

c. A person working in or for the legislative or judicial branches who has been granted access to classified information and the investigation or determination was conducted by the executive branch, but does not include members of Congress, Justices of the Supreme Court, or Federal judges appointed by the President.

d. Covered individuals are not limited to government employees and include all persons, not excluded under paragraphs (a), (b), or (c) of this definition, who have access to classified information or who hold sensitive positions, including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts, consultants, and government employees.

6. "Drugs": Any drug as defined in 21 U.S.C. 321.

7. "Foreign Intelligence Entity": Known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.

8. "Foreign National": Any person who is not a U.S. citizen or a U.S. national.

9. "Media": Any person, organization, or entity, other than Federal, state, local, tribal, and territorial governments:

a. Primarily engaged in the collection, production, or dissemination to the public of information in any form, which includes print, broadcast, film, and Internet; or

b. Otherwise engaged in the collection, production, or dissemination to the public of information in any form related to topics of national security, which includes print, broadcast, film, and Internet.

10. "National Security": Those activities which are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, or terrorism.

11. "National Security Eligibility": Eligibility for access to classified information or eligibility to hold a sensitive position, to include access to sensitive compartmented information, restricted data, and controlled or special access program information.

12. "Sensitive Position": Any position within or in support of an agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on national security regardless of whether the occupant has access to classified information and regardless of whether the occupant is an employee, military service member, or contractor.

13. "Unauthorized Disclosure": A communication, confirmation, acknowledgement, or physical transfer of classified information, including the facilitation of, or actual giving, passing, selling, publishing, or in any way making such information available to an unauthorized recipient.

E. POLICY:

1. All covered individuals incur a special and continuing security obligation to be aware of the risks associated with foreign intelligence operations and/or possible terrorist activities directed against them in the United States and abroad. These individuals also have a responsibility to recognize and avoid personal behaviors and activities that may adversely impact their continued national security eligibility.

2. Covered individuals shall report to their agency head or designee any planned or actual involvement in any of the activities below prior to participation in such activities or otherwise as soon as possible following the start of their involvement. Heads of agencies or designees shall conduct an analysis of such reported activities to determine whether they pose a potential threat to national security and take appropriate action.

3. Failure to comply with reporting requirements and resultant determinations made by the agency may result in administrative action that includes, but is not limited to, revocation of national security eligibility.

4. Heads of agencies or designees may determine that operational and mission needs preclude strict adherence to these reporting requirements. In these instances, equivalent notification, briefing, and reporting shall be accomplished in accordance with agency requirements.

5. Reporting shall be automated to the extent practicable and provide required data elements as identified in Appendix A.

6. Heads of agencies or designees should use available classified and unclassified resources to help determine travel risk, which may include the following:

a. National Counterintelligence and Security Center, National Threat Identification and Prioritization Assessment;

b. Department of State, Security Environment Threat List;

c. Department of State, Travel Alerts and Warnings; and

d. Defense Intelligence Agency Threat List.

7. Heads of agencies may require additional or more detailed reporting and approval procedures for covered individuals under their purview.

8. Covered individuals shall only be required to report to the agency that sponsors their clearance or determined the position they occupy to be sensitive. This does not preclude agency agreements for covered individuals to report to or through a different agency.

F. REPORTABLE ACTIVITIES FOR ALL COVERED INDIVIDUALS:

1. Foreign Travel:

a. Heads of agencies or designees shall determine requirements for reporting foreign travel as part of a covered individual's official duties.

b. Unofficial Foreign Travel:

1) Covered individuals shall submit an itinerary for unofficial foreign travel to their agency head or designee and, except as noted in the subparagraphs below, must receive approval prior to the foreign travel. Unanticipated border crossings into any foreign country not included in the traveler's approved itinerary, regardless of duration, are discouraged. All deviations from approved travel itineraries shall be reported within five business days of return.

a) Travel to Puerto Rico, Guam, or other U.S. possessions and territories is not considered foreign travel and need not be reported.

b) Unplanned day trips to Canada or Mexico shall be reported upon return. Reporting shall be within five business days.

c) When required by the agency head or designee, covered individuals shall, prior to travel, receive a defensive security and counterintelligence briefing.

d) While emergency circumstances may preclude full compliance with pre-travel reporting requirements, the covered individual, at a minimum, shall verbally advise their supervisor/management chain of the emergency foreign travel with all pertinent specifics and, preferably, a security representative, prior to departure. In any event, full reporting shall be accomplished within five business days of return.

e) Consistent with national security, heads of agencies or designees may identify, for covered individuals under their purview, conditions under which prior reporting and approval of unofficial travel is not required, such as, agencies with an overseas presence that may require less specific reporting as opposed to every instance, e.g. travelled to x country y times last month, travel weekly/monthly to x country, travel to x country y times per year, etc.

2) Heads of agencies or designees may disapprove an unofficial foreign travel request when it is determined that such travel presents an unacceptable risk and the physical safety and security of covered individuals or classified information cannot be reasonably ensured. Failure to comply with such disapproval may result in administrative action that includes, but is not limited to, revocation of national security eligibility.

2. Foreign Contacts:

a. Heads of agencies or designees shall determine requirements for reporting contact with a foreign national as part of a covered individual's official duties.

b. Unofficial Contacts:

1) Unofficial contact with a known or suspected foreign intelligence entity.

2) Continuing association with known foreign nationals that involve bonds of affection, personal obligation, or intimate contact; or any contact with a foreign national that involves the exchange of personal information. This reporting requirement is based on the nature of the relationship regardless of how or where the foreign national contact was made or how the relationship is maintained (i.e. via personal contact, telephonic, postal system, Internet, etc.). The reporting of limited or casual public contact with foreign nationals is not required absent any other reporting requirement in this directive. Following initial reporting, updates regarding continuing unofficial association with known foreign nationals shall occur only if and when there is a significant change in the nature of the contact. Heads of agencies or designees may provide specific guidance and examples of updated reporting situations.

3. **Reportable Actions by Others**: To ensure the protection of classified information or other information specifically prohibited by law from disclosure, covered individuals shall alert agency heads or designees to the following reportable activities of other covered individuals that may be of potential security or counterintelligence (CI) concern:

a. An unwillingness to comply with rules and regulations or to cooperate with security requirements.

b. Unexplained affluence or excessive indebtedness.

c. Alcohol abuse.

d. Illegal use or misuse of drugs or drug activity.

e. Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified information or other information specifically prohibited by law from disclosure.

f. Criminal conduct.

g. Any activity that raises doubts as to whether another covered individual's continued national security eligibility is clearly consistent with the interests of national security.

h. Misuse of U.S. Government property or information systems.

4. Covered individuals who have been identified by their respective agency head in accordance with EO 12968, as amended, Section 1.3. (a) shall file a financial disclosure report, as appropriate.

G. REPORTABLE ACTIVITIES FOR INDIVIDUALS WITH ACCESS TO SECRET AND CONFIDENTIAL INFORMATION, "L" ACCESS, OR HOLDING A NON-CRITICAL SENSITIVE POSITION: In addition to the reporting requirements in Section F, individuals with access to Secret and Confidential information, "L" access, or holding a Non-Critical sensitive position shall also report:

1. Foreign Activities:

a. Application for and receipt of foreign citizenship.

b. Application for, possession, or use of a foreign passport or identity card for travel.

2. Other Reportable Activities:

a. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of means.

b. Media contacts, other than for official purposes, where the media seeks access to classified information or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure. Media contacts related to the fulfillment of official duties of the position held by the covered individual need not be reported.

c. Arrests.

d. Bankruptcy or over120 days delinquent on any debt.

e. Alcohol-and drug-related treatment.

H. REPORTABLE ACTIVITIES FOR INDIVIDUALS WITH ACCESS TO TOP SECRET INFORMATION, "Q" ACCESS, OR HOLDING A CRITICAL OR SPECIAL SENSITIVE POSITION: In addition to the reporting requirements in Section F, individuals with access to Top Secret information, "Q" access, or holding a Critical or Special sensitive position shall also report:

1. Foreign Activities:

   a. Direct involvement in foreign business.

   b. Foreign bank accounts.

   c. Ownership of foreign property.

   d. Application for and receipt of foreign citizenship.

   e. Application for, possession, or use of a foreign passport or identity card for travel.

   f. Voting in a foreign election.

   g. Adoption of non-U.S. citizen children.

2. Other Reportable Activities

   a. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of means.

   b. Media contacts where the media seeks access to classified information or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure. Media contacts related to the fulfillment of official duties of the position held by the covered individual need not be reported.

   c. Arrests.

   d. Financial Anomalies: Including, but not limited to, bankruptcy; garnishment; over 120 days delinquent on any debt; and any unusual infusion of assets of $10,000 or greater such as an inheritance, winnings, or similar financial gain.

   e. Foreign National Roommate(s): Any foreign national(s) who co-occupies a residence for a period of more than 30 calendar days.

   f. Cohabitant(s).

   g. Marriage.

   h. Alcohol- and drug-related treatment.

I. RESPONSIBILITIES:

1. The Security Executive Agent will:

   a. Monitor the effectiveness of reporting requirements and develop recommendations for new or modified requirements.

   b. Oversee agency compliance.

   c. Ensure best practices are identified, shared, and implemented.

2. Heads of agencies shall:

   a. Implement the requirements of this directive within 180 days of the date of signature.

b. Develop agency reporting guidance and processes that include the Required Data Elements for Reporting, as provided in Appendix A.

c. Automate and centralize reporting to the extent practicable.

d. Maintain all reported information consistent with applicable law and policy.

e. Ensure policies and procedures governing the collection and use of reported information are in accordance with all applicable laws and executive orders and include appropriate protections for privacy and civil liberties.

f. Analyze, act upon, and share, as appropriate, relevant reported information of a security, counterintelligence (CI), or law enforcement concern with authorized security, CI, insider threat, or law enforcement officials.

g. Share relevant reported information that may result in an adverse determination of the covered individual's continued national security eligibility with security or CI officials of other agencies that have a direct interest in the covered individual. Direct interest is defined as the covered individual being on joint duty, detail, or otherwise working for or within the other agency; or the other agency has granted access or additional access to the covered individual.

h. Provide training and briefing as described in this Directive, to include ensuring awareness of individual reporting obligations, at a minimum, during employee indoctrination and in annual refresher training.

i. Cooperate with the SecEA in assessing the continued efficiency and effectiveness of these and any future reporting requirements.

J. EFFECTIVE DATE: This Directive becomes effective 180 days after the date of signature.

James R. Clapper

Security Executive Agent

14 Dec 2016

Date

APPENDIX A
REQUIRED DATA ELEMENTS FOR REPORTING

When self-reporting or reporting about others is necessary, the following information must be provided in the report, as available and applicable.

1. Foreign travel:
   - **a.** Complete itinerary.
   - **b.** Dates of travel.
   - **c.** Mode of transportation and identity of carriers.
   - **d.** Passport data.
   - **e.** Names and association (business, friend, relative, etc.) of foreign national traveling companions.
   - **f.** Planned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (business, friend, relative, etc.).
   - **g.** Unplanned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (post-travel reporting).
   - **h.** Name, address, telephone number, and relationship of emergency point of contact.
   - **i.** Unusual or suspicious occurrences during travel, including those of possible security or counterintelligence significance (post-travel reporting).
   - **j.** Any foreign legal or customs incidents encountered (post-travel reporting).
2. Unofficial contact with a known or suspected foreign intelligence entity:
   - **a.** Service(s) involved.
   - **b.** Name of individual(s) contacted.
   - **c.** Date(s) of contact.
   - **d.** Nature of contact to include any unusual or suspicious activity.
   - **e.** Likelihood of future contacts.
3. Continuing association with a known foreign national(s) or foreign national roommate(s):
   - **a.** Name of foreign national(s).
   - **b.** Citizenship(s).
   - **c.** Occupation.
   - **d.** Nature of relationship, i.e., business or personal.
   - **e.** Duration and frequency of contact(s).
   - **f.** Current status of the relationship(s).
4. Involvement in foreign business:
   - **a.** Nature of involvement.

b. Countries involved.

c. Name of business.

5. Foreign Bank Account:
   a. Financial institution.
   b. Country.
6. Ownership of foreign property:
   a. Location.
   b. Estimated value.
   c. Balance due.
   d. Purpose and use of property.
   e. How acquired.
7. Foreign citizenship:
   a. Country.
   b. Basis for citizenship.
   c. Date of application or receipt.
8. Application for a foreign passport or identity card for travel:
   a. Country.
   b. Date of application.
   c. Reason for application.
9. Possession of a foreign passport or identity card for travel:
   a. Issuing country.
   b. Number.
   c. Date of issuance.
   d. Expiration date.
   e. Reason for possession.
10. Use of a foreign passport or identity card for travel:
    a. Issuing country.
    b. Reason for use.
    c. Date(s) and country(ies) of use.
11. Voting in a foreign election:
    a. Date.
    b. Country.
    c. Election.

12. Adoption of non-U.S. citizen children:

    a. Country involved.

    b. Foreign government organization involved.

    c. Foreign travel required.

    d. Adoption agency or other intermediary.

    e. Adoptive parents' current linkage to foreign country.

13. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure:

    a. Date(s) of incident.

    b. Name of individual(s) involved.

    c. Nature of incident.

    d. Method of contact.

    e. Electronic address.

    f. Type of information being sought.

    g. Background, circumstances, and current state of the matter.

14. Media contacts:

    a. Date(s) of contact.

    b. Name of media outlet.

    c. Name of media representative.

    d. Nature and purpose of contact.

    e. Whether classified information or other information specifically prohibited by law from disclosure was involved in the contact.

    f. Current status of the contact.

15. Arrests:

    a. Date(s) of the incident(s).

    b. Location(s) of the incident(s).

    c. Charges and/or circumstances.

    d. Disposition.

16. Financial Issues and Anomalies:

    a. Type of issue or anomaly (bankruptcy, inheritance, etc.).

    b. Dollar value.

    c. Reason.

17. Cohabitant(s):

    a. Name(s).

b. Citizenship(s).

c. Date of Birth.

d. Place of Birth.

e. Duration of contact(s).

18. Marriage:

a. Name of spouse.

b. Citizenship of spouse.

c. Date of Birth.

d. Place of Birth.

e. Date of marriage.

19. Alcohol- and drug-related treatment:

a. Reason.

b. Treatment provider, to include contact information.

c. Date(s) treatment provided.

Dear Colleagues:

As we all know, the recent cyber incidents targeting federal government employees' personal information have created potential concerns for many of us, our relatives, and our associates.

We are mindful that the acquisition of personal information can enhance the ability of criminals and foreign governments to target Treasury employees and those closest to us through personal contact or through electronic means, such as by using social media or email. These malicious cyber actors target Treasury employees with motives ranging from the theft of sensitive Treasury information to financially motivated credit card fraud and identity theft.

Mitigating these threats will require our ongoing individual and collective vigilance. Our people are our prize assets. In this vein, please consider carefully the attached guidance from Leslie Ireland, Treasury's Assistant Secretary for Intelligence and Analysis. Secretary Lew and I asked Assistant Secretary Ireland for her thoughts, and we are grateful that she has prepared these helpful cyber and physical security reminders for the Treasury workforce. I encourage you to read it in its entirety and consider how you can incorporate these best practices into your daily lives. Feel free to contact us at 202-622-1348 to continue this discussion.

SBR

Dear Colleagues:

Your identity as a U.S. Government employee and the work you do at the Treasury Department are of great importance, but may also carry with them risk. I write today to urge each of you to take additional steps to reduce your risk in the wake of recent data breaches involving Personally Identifiable Information (PII).

I trust you have already taken steps to protect your identity, by checking your financial accounts regularly and considering identity protection programs. Below you will find a number of steps identified by our security team to help you. To summarize the high points:

- **Everyday Guidance**: Think about your profile as a federal employee and look for ways to minimize risks – for example, by removing your badge and/or parking pass when not at work, sharing only necessary details about your job on publicly accessible social media and networking sites, and using your government email accounts only for official business.

- **Cybersecurity**: Be careful about opening emails from people you do not know and, if you do, be careful about clicking on links or opening attachments. In the wake of the OPM breach, which may have included information about family members and other personal

and business acquaintances, you should pause before opening emails that seem odd, even if appearing to be from people you know.

- **Physical Security:** As a general reminder, maintain good situational awareness. Stay alert and observant for unusual or suspicious behavior or activity. Report suspicious activity to local law enforcement or security authorities.

- **Traveling Overseas:** Whether you are in the United States or abroad, be aware of your surroundings, including the people around you and whether they seem to follow your actions or approach you with unusual questions.

I encourage you to take five minutes to review the following best practices and general guidance, which may help reduce your risk to targeting by potential adversaries, including foreign governments and non-state actors. Please feel free to share this with interested friends and family members.

Immediately report any suspicious activities and contacts, whether experienced by you directly or your family members, using your Bureau's existing security protocols or to Treasury's Office of Counterintelligence at **CI@treasury.gov** or **(202) 622-1348**. For even more helpful information, please see guidance from the National Counterintelligence and Security Center.

Thank you in advance for your vigilance,

S. Leslie Ireland
Assistant Secretary for Intelligence and Analysis

U.S. Department of the Treasury

Everyday Guidance

- Be wary of attempted contact by individuals or groups unknown to you, whether by email, phone, social media, or personal encounters.

- Take care not to broadcast your U.S. Government affiliation outside of work, including on social media sites. Remove your PIV card, parking permit, and other indicators of your federal employment when you depart the building.

- Foreign intelligence officers and other adversaries may seek access to you through a family member. As appropriate, talk with your immediate family members, especially those identified in your records at OPM, and share this same guidance. Ask them to tell you about any suspicious activities and contacts they experience.

- Immediately report any suspicious activities and contacts, whether experienced by you directly or your immediate family members, to your Bureau's security office or Treasury's Office of Counterintelligence at **CI@treasury.gov** or **(202) 622-1348**.

Cybersecurity

- Even when you know the sender of an email, ask yourself if the requested action is consistent with your normal interactions with that person. Always think twice before clicking on links or opening attachments you aren't expecting.

- Be alert to any suspicious activity related to your personal and government-issued electronic devices, such as spam messages from unknown senders or excessive, out-of-cycle, or unusual software downloads or updates.

- Be careful when transmitting personal and work-related information, particularly via phone and web. Metadata in electronic files (including documents and photos) typically contains identifying information, including file creation timestamps and location information. Therefore be attentive to avoid inadvertently disclosing such information. Where appropriate, use secure means to transmit sensitive information.

- Be mindful of the information you post on social media sites. When you have a minute, log out of your social media profiles and try to replicate how someone would access your profiles from the Internet. This will allow you to see what information from your social media profiles is publicly available.

- Make an effort to understand and monitor your privacy and security settings on social media sites. Consider limiting access to your social media profiles to individuals you personally approve.

Physical Security

- As a general reminder, it is always a good idea to maintain good situational awareness. Stay alert and observant for unusual or suspicious behavior or activity.

- As a further general reminder, keep your residence doors and windows secured, even when at home. Do not open your door to anyone until you verify their identity and confirm that they do not pose a threat. Be careful about providing personal information to individuals conducting door-to-door activity, even if it appears to be for a good cause. Familiarize yourself with your neighbors and their vehicles so you can recognize outsiders and unusual vehicles in your neighborhood.

- Remove decals, parking passes, and other visible items from your vehicle that may reveal your identity and place of work or residence. Maintain positive control of keys, badges, or other items that enable access to your car, residence, or place of work.

- Report suspicious activity to local law enforcement or security authorities. If possible, note personal characteristics of suspect individuals and the license plate number, color, and make/model of suspicious vehicles.

- The Department of Homeland Security (DHS) developed the "If You See Something, Say Something" campaign to remind citizens to pay attention and report suspicious activities. Additional information can be found at http://www.dhs.gov/see-something-say-something.

Traveling Overseas

- Be especially vigilant when traveling overseas, whether in your work or personal capacity. You should assume that your affiliation with the U.S. Government is known to the foreign country you are visiting.

- Don't bring sensitive official materials or equipment with you, and don't discuss sensitive official matters.

- Safeguard your personal documents and electronic devices. Consider leaving non-essential personal electronic devices at home and only take government-issued equipment that is intended for overseas use.

- Remember that rental cars or hotel rooms, including hotel room safes, are not secure places to leave sensitive information in print or electronic format.

- Avoid risky behavior or potentially embarrassing situations. Foreign intelligence and security services regularly stage opportunities to create vulnerabilities, monitor and exploit weaknesses, or look for misconduct overseas. This is basic tradecraft to create leverage that can be used to gain sensitive information, including through blackmail, extortion, or coercion.

- If you are approached by anybody seeking sensitive information, please report that contact to Treasury's Office of Counterintelligence at **CI@treasury.gov** or **(202) 622-1348**.

- Know the locations and contact information for U.S. embassies or consulates for any issues or emergencies that might arise when you are overseas. Additional information can be found at http://www.state.gov/travel/index.htm.

POSITION DESCRIPTION NUMBER	POSITION TITLE
04Z502	ACCOUNTANT (SENIOR ACCOUNTANT)
05Z026	ADMINISTRATIVE OFFICER (DEPUTY DIRECTOR)
14013Z	ASSISTANT DIRECTOR, INVESTIGATIVE SUPPORT
Z21820	ASSISTANT INSPECTOR GENERAL FOR AUDIT
Z61180	ASSISTANT INSPECTOR GENERAL FOR AUDIT
Z61197	ASSISTANT INSPECTOR GENERAL FOR AUDIT
10063Z	ASSISTANT INSPECTOR GENERAL FOR AUDIT
Z64034	ASSISTANT INSPECTOR GENERAL FOR INVESTIGATION
Z65009	ASSISTANT INSPECTOR GENERAL FOR INVESTIGATIONS
17007Z	AUDITOR
Z29958	AUDITOR
Z29973	AUDITOR
Z30009	AUDITOR
Z30010	AUDITOR
08006Z	BUDGET ANALYST
16022Z	CHIEF INFORMATION OFFICER
15014Z	CONTRACT SPECIALIST
Z61181	COUNSEL TO THE INSPECTOR GENERAL
02Z356	CRIMINAL INVESTIGATOR
03Z310	CRIMINAL INVESTIGATOR
04Z304	CRIMINAL INVESTIGATOR
04Z307	CRIMINAL INVESTIGATOR
05Z012	CRIMINAL INVESTIGATOR
06Z406	CRIMINAL INVESTIGATOR
09016Z	CRIMINAL INVESTIGATOR
10078Z	CRIMINAL INVESTIGATOR
10079Z	CRIMINAL INVESTIGATOR
10099Z	CRIMINAL INVESTIGATOR

16017Z	CRIMINAL INVESTIGATOR
16028Z	CRIMINAL INVESTIGATOR
17008Z	CRIMINAL INVESTIGATOR
Z29924	CRIMINAL INVESTIGATOR
Z29943	CRIMINAL INVESTIGATOR
Z90706	CRIMINAL INVESTIGATOR
Z90707	CRIMINAL INVESTIGATOR
Z91083	CRIMINAL INVESTIGATOR
Z91084	CRIMINAL INVESTIGATOR
Z91085	CRIMINAL INVESTIGATOR
Z91086	CRIMINAL INVESTIGATOR
Z91436	CRIMINAL INVESTIGATOR
16025Z	CRIMINAL INVESTIGATOR (SENIOR SPECIAL AGENT)
15227Z	CRIMINAL INVESTIGATOR, SENIOR SPECIAL AGENT)
10086Z	DEPUTY COUNSEL TO THE INSPECTOR GENERAL FOR TAX ADMINISTRATION
Z61054	DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS
Z61003	DEPUTY INSPECTOR GENERAL
15213Z	DIRECTOR, ENTERPRISE ARCHITECTURE & INFORMATION TECHNOLOGY
05Z006	DIRECTOR, FORENSIC LABORATORY
14003Z	DIRECTOR, STRATEGIC DATA SERVICES
Z25792	FINGERPRINT SPECIALIST (SENIOR)
Z87356	FORENSIC DOCUMENT ANALYST
14018Z	HUMAN RESOURCES SPECIALIST
Z30060	HUMAN RESOURCES SPECIALIST
04Z609	INFORMATION TECHNOLOGY SPECIALIST
14006Z	INFORMATION TECHNOLOGY SPECIALIST
15204Z	INFORMATION TECHNOLOGY SPECIALIST
16037Z	INFORMATION TECHNOLOGY SPECIALIST
14009Z	INFORMATION TECHNOLOGY SPECIALIST
Z30043	INFORMATION TECHNOLOGY SPECIALIST
05Z008	INSPECTOR GENERAL
10064Z	INVESTIGATIVE ANALYST

10065Z	INVESTIGATIVE ANALYST
10100Z	INVESTIGATIVE ANALYST
14012Z	INVESTIGATIVE ANALYST
14014Z	INVESTIGATIVE ANALYST
15012Z	INVESTIGATIVE ANALYST
15013Z	INVESTIGATIVE ANALYST
15233Z	INVESTIGATIVE ANALYST (CYBERCRIMES)
04Z308	INVESTIGATIVE SPECIALIST
10112Z	INVESTIGATIVE SPECIALIST
Z30035	INVESTIGATIVE SPECIALIST
Z30036	INVESTIGATIVE SPECIALIST
Z36392	INVESTIGATIVE SPECIALIST
10069Z	IT SPECIALIST (INFOSEC)
10071Z	IT SPECIALIST (INFOSEC)
02Z333	LEAD FINGERPRINT SPECIALIST
02Z332	LEAD FORENSIC DOCUMENT ANALYST
16032Z	LEAD PERSONNEL SECURITY SPECIALIST
10083Z	MANAGEMENT ANALYST
10123Z	MANAGEMENT ANALYST
Z30051	MANAGEMENT ANALYST
03Z406	MANAGEMENT AND PROGRAM ANALYST
09002Z	MANAGEMENT AND PROGRAM ANALYST
10092Z	MANAGEMENT AND PROGRAM ANALYST
10094Z	MANAGEMENT AND PROGRAM ANALYST
13006Z	MANAGEMENT AND PROGRAM ANALYST
13011Z	MANAGEMENT AND PROGRAM ANALYST
Z92174	MANAGEMENT AND PROGRAM ANALYST
08020Z	PERSONNEL SECURITYSPECIALIST
10091Z	PROGAM ANALYST
02Z543	PROGRAM & MANAGEMENT ANALYST
02Z358	PROGRAM ANALYST
05Z015	PROGRAM ANALYST

08014Z	PROGRAM ANALYST
09010Z	PROGRAM ANALYST
09033Z	PROGRAM ANALYST
10059Z	PROGRAM ANALYST
10089Z	PROGRAM ANALYST
10113Z	PROGRAM ANALYST
11153Z	PROGRAM ANALYST
12155Z	PROGRAM ANALYST
12170Z	PROGRAM ANALYST
14025Z	PROGRAM ANALYST
Z29934	PROGRAM ANALYST
Z30048	PROGRAM ANALYST
07017Z	PROGRAM ANALYST (AUDIT EVALUATOR)
11130Z	PROGRAM ASSISTANT
08004Z	PROGRAM MANAGER
09013Z	PROGRAM MANAGER
09014Z	PROGRAM MANAGER
10119Z	PROGRAM MANAGER
05Z010	PROGRAM MANAGER
04Z107	PUBLIC AFFAIRS SPECIALIST
10060Z	PUBLIC AFFAIRS SPECIALIST
06Z404	QUALITY MANAGER FOR FORENSIC SCIENCE LAB
05Z018	SECRETARY
Z30058	SECRETARY
09005Z	SECRETARY
Z30059	SECRETARY
16020Z	SECURITY OFFICER (ASSISTANT DIRECTOR)
07019Z	SPECIAL AGENT - SYSTEM INTRUSION & NET
08011Z	SPECIAL AGENT - SYSTEM INTRUSION & NET
06Z411	STAFF ASSISTANT
06Z412	STAFF ASSISTANT
09022Z	STAFF ASSISTANT

09042Z	STAFF ASSISTANT
09051Z	STAFF ASSISTANT
02Z446	STUDENT TRAINEE (AUDITING)
03Z404	SUPERVISORY AUDITOR
03Z408	SUPERVISORY AUDITOR
11147Z	SUPERVISORY AUDITOR
Z29952	SUPERVISORY AUDITOR
Z91509	SUPERVISORY AUDITOR
09041Z	SUPERVISORY AUDITOR (DIRECTOR)
10084Z	SUPERVISORY AUDITOR (DIRECTOR)
13016Z	SUPERVISORY BUDGET ANALYST
11145Z	SUPERVISORY CONTRACT SPECIALIST
07027Z	SUPERVISORY CRIMINAL INVESTIGATOR
Z29944	SUPERVISORY CRIMINAL INVESTIGATOR
Z29947	SUPERVISORY CRIMINAL INVESTIGATOR
06Z402	SUPERVISORY FINANCIAL MANAGER
Z29914	SUPERVISORY GENERAL ATTORNEY
15203Z	SUPERVISORY INFOTECHNOLOGY SPECIALIST
03Z606	SUPERVISORY IT SPECIALIST
11135Z	SUPERVISORY IT SPECIALIST
15219Z	SUPERVISORY IT SPECIALIST
16040Z	SUPERVISORY IT SPECIALIST
16023Z	SUPERVISORY IT SPECIALIST (CUSTSPT)
16039Z	SUPERVISORY IT SPECIALIST (INFOSEC)
13008Z	SUPERVISORY MANAGEMENT & PROGRAM ANALYST
08032Z	SUPERVISORY MANAGEMENT AND PROGRAM ANALYST
06Z405	SUPERVISORY PROGRAM ANALYST
08007Z	SUPERVISORY PUBLIC AFFAIRS SPECIALST
09011Z	TECHNICAL ASSISTANT
09017Z	VISUAL INFORMATION SPECIALIST
10053Z	WRITER/EDITOR

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

June 27, 2017

TIGTA #17-25
MEMORANDUM FOR TIGTA MANAGERS

FROM: Mervin Hyndman
Acting Deputy Inspector General for Mission Support/
Chief Financial Officer

SUBJECT: Mandatory Drug-Free Workplace Training

As mandated by Executive Order (EO) 12564, Drug-Free Federal Workplace, all agencies are to provide mandatory training to all supervisors to assist in addressing agency employee illegal drug use. Further, agencies are also required to report the number of supervisors who have completed this training.

To ensure compliance with this EO, the Office of Mission Support Leadership and Human Capital Directorate will continue to provide training for all Treasury Inspector General for Tax Administration (TIGTA) supervisors. This training will enhance TIGTA supervisors' awareness of the EO and the Governmentwide effort demonstrating that illegal drugs will not be tolerated in the Federal workplace.

If you are a recipient of this notice, you are required to complete the *TIGTA Drug-Free Workplace Training for Supervisors* by **Friday, July 14, 2017**. This training has been assigned to you via the Treasury Learning Management System (TLMS).

If you have any questions about this requirement, please contact TIGTA Drug-Free Workplace mailbox at tigtadfwp@tigta.treas.gov. For TLMS assistance, please contact the TLMS Helpdesk at (304) 480-8000, option 4, or your function's TLMS Administrator.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

June 7, 2017

TIGTA #17-24
MEMORANDUM FOR ALL EMPLOYEES

FROM: Mervin Hyndman
Acting Deputy Inspector General for Mission Support/Chief Financial Officer

SUBJECT: Mandatory Training on Privacy Awareness and Information Privacy

As Treasury Inspector General for Tax Administration (TIGTA) employees, we know the important role our organization plays in the detection and prevention of unauthorized access or inspection of confidential information, including tax returns and return information. In addition, we are all responsible for safeguarding records and information that we use in connection with performing our duties and responsibilities as TIGTA employees. In recognition of the importance of safeguarding the confidentiality of Agency records, TIGTA employees are required to complete TIGTA's Information Privacy Briefing which discusses our authority under I.R.C. § 6103 and the Privacy Act to access and disclose confidential Agency records. **At the conclusion of the training, each employee will be required to take a test and obtain a minimum score of 80 percent to obtain a passing grade and receive credit for the course.** Employees are required to retake the test until they obtain a minimum score of 80 percent.

Each employee is responsible for completing the training by **June 30, 2017**. Employees may access the briefing on the Treasury Learning Management System (TLMS) website at https://tlms.treas.gov/. Employees will be allowed up to one (1) hour to review the training material and take the test. Additionally, employees with questions about this briefing should contact counsel.office@tigta.treas.gov or call (202) 622-4068. Employees needing TLMS assistance should contact the TLMS Helpdesk at 304-480-8000, option 4 or their functional TLMS Administrator.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

May 9, 2017

TIGTA #17-23
MEMORANDUM FOR ALL TIGTA MANAGERS

FROM: Mervin Hyndman
Acting Deputy Inspector General for Mission Support/
Chief Financial Officer

SUBJECT: Mandatory Veterans Training

Executive Order (EO) 13518, *Employment of Veterans in the Federal Government*, requires all agencies to provide mandatory annual training to human resources personnel and hiring managers concerning veterans' employment, including training on veterans' preferences and special authorities for the hiring of veterans. Further, agencies must report the number of required employees who have completed the training.

To ensure compliance with this EO, the Office of Mission Support Leadership and Human Capital Directorate previously added two mandatory training courses for all Treasury Inspector General for Tax Administration (TIGTA) managers' "To Do List" in the Treasury Learning Management System (TLMS). The two mandatory courses are: *Uniformed Services Employment and Reemployment Rights Act FY17*; and *Veteran Employment Training for Federal Hiring Managers FY17*. This training will enhance TIGTA managers' awareness of this EO and the Government-wide effort to increase the number of veterans employed by the Federal Government.

Please complete the required training by **Friday, July 14, 2017**. Managers are also responsible for ensuring their employees, who are involved in TIGTA hiring activities, complete the training by the required due date.

If you have any questions about his requirement, please contact Leadership & Human Capital via mailbox *TIGTA OMS Human Capital. Also, if a TIGTA employee has training access issues or needs TLMS assistance, please contact the TLMS Helpdesk at (304) 480-8000, option 4, or your function's TLMS Administrator.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

May 11, 2017

TIGTA #17-22
MEMORANDUM FOR ALL TIGTA EMPLOYEES

B Woolfolk

FROM: Brittany M. Woolfolk
Equal Employment Opportunity Program Manager

SUBJECT: Annual Mandatory No FEAR Act and Diversity Training

The *Notification and Federal Employee Antidiscrimination and Retaliation Act*, enacted in 2002 and commonly known as the *No FEAR Act*, requires Federal agencies to be accountable for violations of antidiscrimination and whistleblower protection laws. It also requires Federal employees to receive biannual training on the provisions of the law. Online training is again being provided in 2017. This training is mandatory for all employees.

The No FEAR Act course can be found on the Treasury Learning Management System (TLMS) at https://tlms.treas.gov/. To access the training, type the course title, "*The No FEAR Act*", in the "Search Catalog" browse button.

In accordance with the Treasury Inspector General for Tax Administration (TIGTA) Strategic Diversity and Inclusion Plan (SDIP) all executives, supervisors, managers and employees should complete mandatory annual diversity training. One section of the SDIP, Workplace Inclusion, Priority 2.2, includes strategies for cultivating a supportive, welcoming, inclusive and fair work environment. In line with this priority is a requirement to provide annual diversity training.

Many employees have attended the Special Emphasis month lunch and learns held in FY2017. If you attended one of these events, you have fulfilled your mandatory diversity training requirement. If you have not attended a lunch and learn you will need to complete a diversity course on TLMS.

This year all employees are required to complete *"Your Role in Workplace Diversity"*. The diversity course can be found on TLMS at https://tlms.treas.gov/. To access the training, type the course title, *"Your Role in Workplace Diversity"*, in the "Search Catalog" browse button.

TIGTA function training coordinators will monitor their employee's participation and ensure that their employees have satisfied the mandatory diversity training requirement by September 8, 2017.

Employees who have questions about accessing this training or who need TLMS assistance should contact their functional TLMS administrator or the TLMS Helpdesk at (304) 480-8000, option 4. If there are any other questions, please contact the EEO office at *TIGTA EEO Requests.

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

May 1, 2017

TIGTA #17-21
MEMORANDUM FOR ALL TIGTA EMPLOYEES

FROM: George J. Jakabcin

Chief Information Officer (CIO)

SUBJECT: Mandatory Cybersecurity Awareness Training

The Federal Information Security Management Act (FISMA) requires all users of Treasury's information systems, including contractor employees, to complete annual cybersecurity awareness training. The threat continues to rise. As stewards of sensitive information and the target of some activity, we need to be better armed to deal with the changing attempts to penetrate, steal, and in some instances damage our information technology capabilities. This year, Treasury has selected a new course that will provide you with the most current and informative training content available.

TIGTA employees will complete this training through the Treasury Learning Management System (TLMS). The training course, "***Annual Cybersecurity Awareness Training***" (*TLMS Course ID: TREAS_SANS_Info_SEC_Awareness*), has been added to each employees' Learning Plan. Employees with questions about accessing this training or needing TLMS assistance should contact their functional TLMS Administrator.

Completion of the Cybersecurity Awareness Training is mandatory and should take approximately two hours. To receive credit for the training, employees must complete all modules. **The training must be completed no later than Thursday, June 1, 2017.** Managers are responsible for ensuring their employees and contractors with TIGTA accounts complete the training by the due date.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

January 10, 2017

TIGTA #17-16
MEMORANDUM FOR ALL TIGTA EMPLOYEES

FROM: Gladys M. Hernández
Chief Counsel

SUBJECT: TIGTA Employee Tax Obligations and
Prohibited Outside Employment – Tax Matters

As the Federal tax filing season approaches, it is time again to remind all Treasury Inspector General for Tax Administration (TIGTA) employees of their obligation to file and pay their Federal, State and local income taxes timely and accurately. 5 C.F.R. § 2635.809. Due to the unique role we play overseeing the Internal Revenue Service (IRS) and the Federal system of tax administration, it is critical that each and every TIGTA employee fulfills his or her personal tax responsibilities. Failure to meet your tax obligations could result in disciplinary action. In some situations, particularly if you willfully fail to file a return, you can be removed from TIGTA employment.

To assist you, here are a few helpful tips to remember:

- File your return by the due date of Tuesday, April 18, 2017.[1] This deadline applies to everyone regardless of whether you owe taxes or expect a refund.
- TIGTA employees may file for an automatic filing extension— which is also due by April 18, 2017. But remember, an extension is only for filing; even with an extension, **you must still estimate and pay any tax you owe by April 18th**.
- File an accurate return by making sure you take into account all sources of taxable income, allowable credits and deductions.

[1] The regular federal tax return filing deadline is April 15. However, due to April 15 being on a Saturday and the Washington D.C. Emancipation Day holiday being observed on Monday, April 17 (instead of April 16, 2017), Tax Day is on the following Tuesday, April 18, 2017.

Section 1203(b) of the Internal Revenue Service Restructuring and Reform Act of 1998 identifies certain acts or omissions and associated penalties related to tax compliance by IRS employees. Pursuant to TIGTA policy, the willful acts or omissions and associated penalties specified in § 1203(b) are applicable to TIGTA employees. Two of these specific willful acts or omissions are as follows:

- Willful failure to file any return required under the Internal Revenue Code on or before the date prescribed therefor (including extensions), unless such failure is due to reasonable cause and not subject to willful neglect;

- Willful understatement of Federal tax liability, unless such understatement is due to reasonable cause and not willful neglect.

For more information on the nine willful acts or omissions, please consult TIGTA Operations Manual, Chapter 600, 70.8.1.3, Section 1203(b) Misconduct – TIGTA Mirror Provisions and Penalties.

To ensure that TIGTA employees are fulfilling their Federal tax responsibilities, TIGTA has implemented an Employee Tax Compliance (ETC) Program. For the ETC Program procedures and other information regarding TIGTA's ETC Program, please consult TIGTA Operations Manual, Chapter (700)-150, *Employee Tax Compliance*.

Please plan ahead and get the assistance you need to uphold your obligation to comply with the law. If you become aware that you may have a tax compliance problem, talk with your manager immediately.

Outside Employment Involving Tax Matters

We also want to remind you that pursuant to the Supplemental Standards of Ethical Conduct for Employees of the Treasury, set forth at 5 CFR § 3101.106, TIGTA Employees are prohibited from the following types of outside employment or business activities (constituting a conflict with the employee's official duties):

(1) Performance of legal services involving Federal, State or local tax matters;[2]

---

[2] Tax matters does not include unpaid (*i.e.*, no compensation, gift, or favor) return preparation or return preparation assistance (*e.g.*, as a VITA volunteer, for a non-profit, or for family members or friends).

(2) Appearing on behalf of any taxpayer as a representative before any Federal, State, or local government agency, in an action involving a tax matter except on written authorization of the Treasury Inspector General for Tax Administration;

(3) Engaging in accounting, or the use, analysis, and interpretation of financial records when such activity involves tax matters;

(4) Engaging in bookkeeping, the recording of transactions, or the record-making phase of accounting, when such activity is directly related to a tax determination; and

(5) Engaging in the preparation of tax returns for compensation, gift, or favor.

Additionally, TIGTA employees also may not recommend, refer, or suggest, specifically or by implication, any attorney, accountant or firm of attorneys or accountants to any person in connection with any official business which involves or may involve the IRS.

TIGTA employees must receive prior approval for any outside employment or business activity, whether compensated or not, involving tax preparation or activities involving tax representation. See TIGTA Operations Manual, Chapter 700, 30.3, Outside Employment Activities.

Thank you for your help in upholding TIGTA's longstanding tradition of high tax compliance standards. If you have any question whether the outside employment or business activity would result in a conflict, please seek further advice from the Office of Chief Counsel prior to engaging in the activity. You may contact the Office of Chief Counsel at (202) 622-4068 or Counsel.Office@tigta.treas.gov.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

January 10, 2017

TIGTA #17-15
MEMORANDUM FOR ALL TIGTA EMPLOYEES

FROM: Gladys M. Hernández
Chief Counsel and Designated Ethics Officer

SUBJECT: Hatch Act Restrictions for Federal Employees

This memorandum provides Counsel's annual reminder to employees regarding the restrictions placed on the political activity of Federal government employees by the Hatch Act.

The Hatch Act places restrictions on the political activities of federal employees based on their classification; most TIGTA employees fall into the "less restricted" class of employees. The general rules for most TIGTA employees[1] are summarized as follows, and apply to the use of email and social media, including Facebook and Twitter:[2]

You MAY:

- register and vote as you choose
- assist in voter registration drives
- express opinions about candidates and issues, including on Facebook and Twitter
- attend fundraisers and contribute money to political organizations and campaigns
- attend and be active at political rallies and meetings

---

[1] The scope of permissible political activity for career members of the Senior Executive Service and certain Presidentially-appointed, Senate-confirmed employees is more limited. Please click on the following link for a list of examples of both permissible and prohibited activities for these employees: Political Activity Guidelines for Federal Employees Subject to the Greatest Restrictions.

[2] For additional guidance concerning the use of email and social media, please click on the following link for a set of Frequently Asked Questions: The Hatch Act: Frequently Asked Questions on Federal Employees and the Use of Social Media and Email.

- join and be an active member of a political party or club
- sign nominating petitions
- campaign for or against referendum questions, constitutional amendments, municipal ordinances
- make campaign speeches for candidates in partisan elections
- distribute campaign literature in partisan elections
- hold office in political clubs or parties
- be a candidate for public office in nonpartisan elections

You MAY NOT:

- use official authority or influence to interfere with an election
- solicit or discourage political activity of anyone with business before your agency
- solicit or receive political contributions, including sharing links to the political contribution page of any partisan group or candidate in a partisan race, or "liking," "sharing," or "retweeting" a solicitation from one of those entities, including an invitation to a political fundraising event
- be a candidate for public office in a partisan election[3]
- engage in political activity (including political activity on Facebook or Twitter) while on duty, in a government office, wearing an official uniform and/or using a government vehicle
- wear partisan political buttons on duty

If you are considering engaging in any political activity please click on the following links for additional information from the Office of Special Counsel, the Federal agency charged with enforcing the Hatch Act, and the Department of the Treasury. We encourage you to contact the Office of Chief Counsel at (202) 622-4068 or by email at *TIGTA Counsel Office for a written opinion regarding whether your proposed political activity is permitted under the Hatch Act.

---

[3] In certain designated communities, including the Washington D.C. suburbs, an employee may run for office in a local partisan election (but only as an independent candidate) and may receive (but not solicit) contributions. *See generally* 5 C.F.R. Part 733.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

January 9, 2017

TIGTA #17-14

MEMORANDUM FOR ALL TIGTA EMPLOYEES

FROM: Gladys M. Hernández
Chief Counsel and Designated Ethics Officer

SUBJECT: Presidential Inaugural Events

The Presidential Inauguration is always surrounded by events like the Inaugural Parade, Inaugural Balls, and other receptions and dinners, making it a good time for a reminder of the gift rules applicable to executive branch employees. Please keep the following in mind if you are considering attending Inaugural events:

- You can attend events or accept items that are free to the public, or if you pay the market value for admission or for the item.

- You can accept gifts from Federal government entities, or from employees acting on their behalf (like from a congressional representative or an official Inaugural committee).

- You can accept gifts that are worth $20 or less combined per occasion, up to $50 in total value in a calendar year. This includes free attendance at a reception or event where the value of your food, drink, and entertainment is $20 or less. **If an event is ticketed, the value of attendance is the face value on the ticket.**

- You can accept gifts from a family member or personal friend. For example, if your spouse's employer gave its employees free tickets to an Inauguration event, you can accept one of the tickets from your spouse.

- You can accept benefits from a political organization if they are in connection with you taking an active part in political management or in a political campaign. For example, if you campaigned for a party or candidate, the party's national committee or the candidate's federally-registered committee can give you free travel and attendance at events.

- You can also accept free attendance at a widely-attended gathering if an agency ethics officer makes a written finding that the agency's interest in you attending the event outweighs the concern of you being improperly influenced in your official duties.

- Finally, even if one of the above situations applies to you, **you should always decline a gift if you determine that a reasonable person, knowing all the facts, would question your integrity or impartiality if you accepted it**. In evaluating whether you may accept a gift, think about the value of the gift, the timing of the offer, the identity of the donor, and whether the gift would give the donor significantly disproportionate access.

You may click on the following link for additional information from the Office of Government Ethics, the Federal agency that oversees the executive branch ethics program. If you receive an offer of free attendance to an Inauguration-related event, we encourage you to contact the Office of Chief Counsel at (202) 622-4068 or by email at *TIGTA Counsel Office if you are unsure whether you may accept it under the ethics gift rules.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

November 4, 2016

TIGTA #17-10
MEMORANDUM FOR ALL TIGTA MANAGERS

FROM: Mervin Hyndman
Acting Deputy Inspector General for Mission Support/
Chief Financial Officer

SUBJECT: Domestic Violence, Sexual Assault, and Stalking Training

In accordance with the Presidential Memorandum on "Establishing Policies for Addressing Domestic Violence in the Federal Workforce," all agencies are required to provide training to its employees on Domestic Violence, Sexual Assault and Stalking (DVSAS). Further, agencies are also required to report the number of employees who have completed the training.

To ensure compliance with this Presidential Memorandum, the Office of Mission Support Leadership and Human Capital Directorate has added the mandatory training course "Domestic Violence, Sexual Assault, and Stalking in the Workplace" to all Treasury Inspector General for Tax Administration (TIGTA) managers' "To Do List" in the Treasury Learning Management System (TLMS). This training is designed to provide guidance and tips on the sensitive and difficult topics related to managing a domestic violence, sexual assault, or stalking matter in the workplace. Among other things, this course will provide information on the definitions and types of DVSAS, how DVSAS is a workplace issue, possible signs and symptoms of DVSAS, confidentiality in the workplace, and identifying the internal and external resources available to assist employees and managers.

Please complete the required training by **Monday, December 5, 2016**. Managers are also responsible for ensuring their employees complete the training by the required due date.

If you have any questions about this requirement, please contact Leadership & Human Capital via mailbox *TIGTA OMS Human Capital. Also, if an employee has training access issues or needs TLMS assistance, please contact the TLMS Helpdesk at (304) 480-8000, option 4, or your function's TLMS Administrator.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

November 1, 2016

TIGTA #17-09
MEMORANDUM FOR ALL TIGTA EMPLOYEES

FROM: Mervin Hyndman
Acting Deputy Inspector General for Mission Support/
Chief Financial Officer

SUBJECT: Annual Outside Employment or Business Activity
Filing Requirement

TIGTA employees seeking to engage in outside employment or business activities are required to obtain prior written approval before engaging in such activity, unless the activity falls under a specific exception as outlined in TIGTA Operations Manual (700)-30.0, by submitting a Form 7995, Outside Employment or Business Activity Request, electronically to the Office of Chief Counsel through the employee's manager prior to engaging in such activity.

Pursuant to the Standards of Ethical Conduct for Executive Branch Employees, 5 C.F.R. §§ 2635.801-809, an employee may not engage in outside employment activity that conflicts with the official duties of his or her position. An activity conflicts with official duties if it is either prohibited by statute or regulation or the activity would require the employee to be disqualified from matters so central to the performance of the employee's official duties as to materially impair the ability to carry out those duties.

The Supplemental Standards of Ethical Conduct for Employees of the Department of the Treasury (Treasury Supplemental Standards), 5 C.F.R. § 3101.104, requires Treasury employees to obtain prior written approval before engaging in any outside employment or business activity (unless exempted), with or without compensation. In addition, the Treasury Supplemental Standards specifically prohibit TIGTA employees from the following types of outside employment or business activities (constituting a conflict with the employee's official duties): (1) Performance of legal services involving Federal, State or local tax matters ("tax matters" does not include unpaid (*i.e.*, no compensation, gift, or favor) return preparation or return preparation assistance (*e.g.*, as a VITA volunteer, for a non-profit, or for family members or friends)); (2) Appearing on behalf of any taxpayer as a representative before any Federal, State, or local

government agency, in an action involving a tax matter except on written authorization of the Commissioner of Internal Revenue or the Treasury Inspector General for Tax Administration; (3) Engaging in accounting, or the use, analysis, and interpretation of financial records when such activity involves tax matters; (4) Engaging in bookkeeping, the recording of transactions, or the record-making phase of accounting, when such activity is directly related to a tax determination; and (5) Engaging in the preparation of tax returns for compensation, gift, or favor. 5 C.F.R. § 3101.106(b). TIGTA employees must obtain prior approval for any activities involving tax preparation or tax representation. TIGTA employees also may not recommend, refer, or suggest, specifically or by implication, any attorney, accountant or firm of attorneys or accountants to any person in connection with any official business which involves or may involve the Internal Revenue Service. 5 C.F.R. § 3101.106(a). If an employee has any question whether the outside employment or business activity would result in a conflict, he or she should seek further advice from the Office of Chief Counsel prior to engaging in the activity.

TIGTA employees who have previously received written approval to engage in outside employment or business activity are reminded that requests for written approval of such employment or activity must be submitted to his or her manager annually, on an **annual and calendar year basis**. Calendar year 2016 approved requests expire on December 31, 2016. Accordingly, employees currently engaged in or wishing to start an outside employment or business activity (not exempted from the filing requirement) must electronically submit a Form 7995, Outside Employment or Business Activity Request, to the Office of Chief Counsel through his or her manager prior to engaging in such activity during Calendar Year 2017. Employees cannot engage in outside employment without a current approved request and must ensure that any outside employment request on file reflects current outside employment. The Office of Chief Counsel will maintain on file all outside employment requests and will return a copy of the approved or disapproved request to the employee and his or her manager.

Employees with questions regarding whether an outside employment or business activity requires prior written approval should consult with TIGTA Counsel at (202) 622-4068 or *TIGTA Counsel Office.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

November 3, 2016

TIGTA #17-08
MEMORANDUM FOR ALL TIGTA EMPLOYEES

FROM: Mervin Hyndman
Acting Deputy Inspector General for Mission Support/
Chief Financial Officer

SUBJECT: Use or Lose Annual Leave

The purpose of this memorandum is to remind all Treasury Inspector General for Tax Administration (TIGTA) employees of the provisions under which annual leave may be restored. The Federal leave year ends on **January 7, 2017.** All use or lose annual leave must be scheduled and approved ***before November* 26, 2016**.

It is the responsibility of all TIGTA employees to review their annual leave balances and schedule excess leave accordingly. Excess hours are reflected in the projected use or lose area located at the lower section of the employee's earnings and leave statement that is available to employees on-line, via the National Finance Center's Employee Personnel Page (EPP). Employees may refer to the EPP website available at https://www.nfc.usda.gov/personal/. The information is also available on the employee's Time and Attendance Summary page under the Leave Year Projection section in the WebTA timekeeping system. TIGTA managers may retrieve this information from timekeepers.

General Schedule (GS) employees, both full- and part-time, may accumulate and carry over, from one leave year to the next, up to a maximum of 240 hours. Senior Executive Service (SES) employees may accumulate and carry over up to 720 hours. Any annual leave at the end of the leave year that exceeds the maximum accumulation is forfeited, unless it meets the criteria for restoration.

Forfeited annual leave for all employees, including members of the SES, may only be restored under the following conditions:

- When annual leave is requested and approved through WebTA no later than **November 26, 2016**, but its use is subsequently denied due to exigency of the public business. Exigency is defined as an urgent situation that would affect the mission of the employee's function; or

- When use of scheduled annual leave is prevented by illness of the employee, provided the annual leave was requested and approved through WebTA no later than **November 26, 2016**, and its use could not be rescheduled between the termination of the illness and the end of the leave year, **January 7, 2017**.
- Annual leave lost due to administrative error will also be restored to the employee.

If these conditions are met, leave restoration may be requested through the employee's immediate manager by preparing a Public Debt Form 5346E, Request for Restoration of Annual Leave, by February 24, 2017. (This form can be accessed at https://arc.publicdebt.treas.gov/fsforms/fs5346.pdf.) The request should provide justification to restore leave including a reason for denial or cancellation of the leave.

Attached to this form should be the following:

- Copies of the WebTA leave request documenting the leave being requested and approved **before** November 26, 2016; and
- Copies of the supervisor's denial or cancellation of leave through WebTA including remarks documenting the reason for cancellation (business exigency) **after** November 26, 2016.

The appropriate function head will make the final decision on all leave restoration requests. **Note: Based on the Code of Federal Regulations, leave must be forfeited before it can be restored. Forfeiture will not occur until the new leave year begins. Therefore, please submit requests to restore annual leave after January 7, 2017. Approved Forms 5346E and the supporting documentation must be received in the Bureau of the Fiscal Service's Pay and Leave Services Branch by February 24, 2017**. Approved requests can be faxed to (304) 480-8295 or e-mailed to Payroll@fiscal.treasury.gov. Copies of leave requests reflecting that leave was requested and approved prior to November 26, 2016 should be attached. All requests submitted without complete documentation will be returned.

Timekeepers should contact the Pay and Leave Services Branch for further direction on how to restore the leave in WebTA. Restored leave must be used within two years of the end of the leave year in which it was restored.

For additional guidance on time and leave, including use or lose annual leave, please refer to TIGTA's Operation Manual, **(600)-70.4 Time and Leave**.

Donating Use or Lose Annual Leave

The Voluntary Leave Transfer Program allows employees to donate annual leave to an employee who needs the leave due to a medical emergency. TIGTA employees with "use or lose" annual leave have the option of donating leave to an approved leave recipient in the Voluntary Leave Transfer Program. An employee may donate to any approved leave recipient with the exception of the employee's immediate manager.

Specifically, employees may donate the lesser of half the annual leave earned during the leave year the donation is made, or the number of hours remaining in the leave year (as of the date of the leave donation) that the employee is scheduled to work and receive pay.

Questions about "use or lose" annual leave, leave transfer or leave restoration, may be directed to the Bureau of the Fiscal Service's Pay and Leave Services Branch at (304) 480-8400 or Payroll@fiscal.treasury.gov. Also, you may contact Leadership and Human Capital at *TIGTA OMS Human Capital.