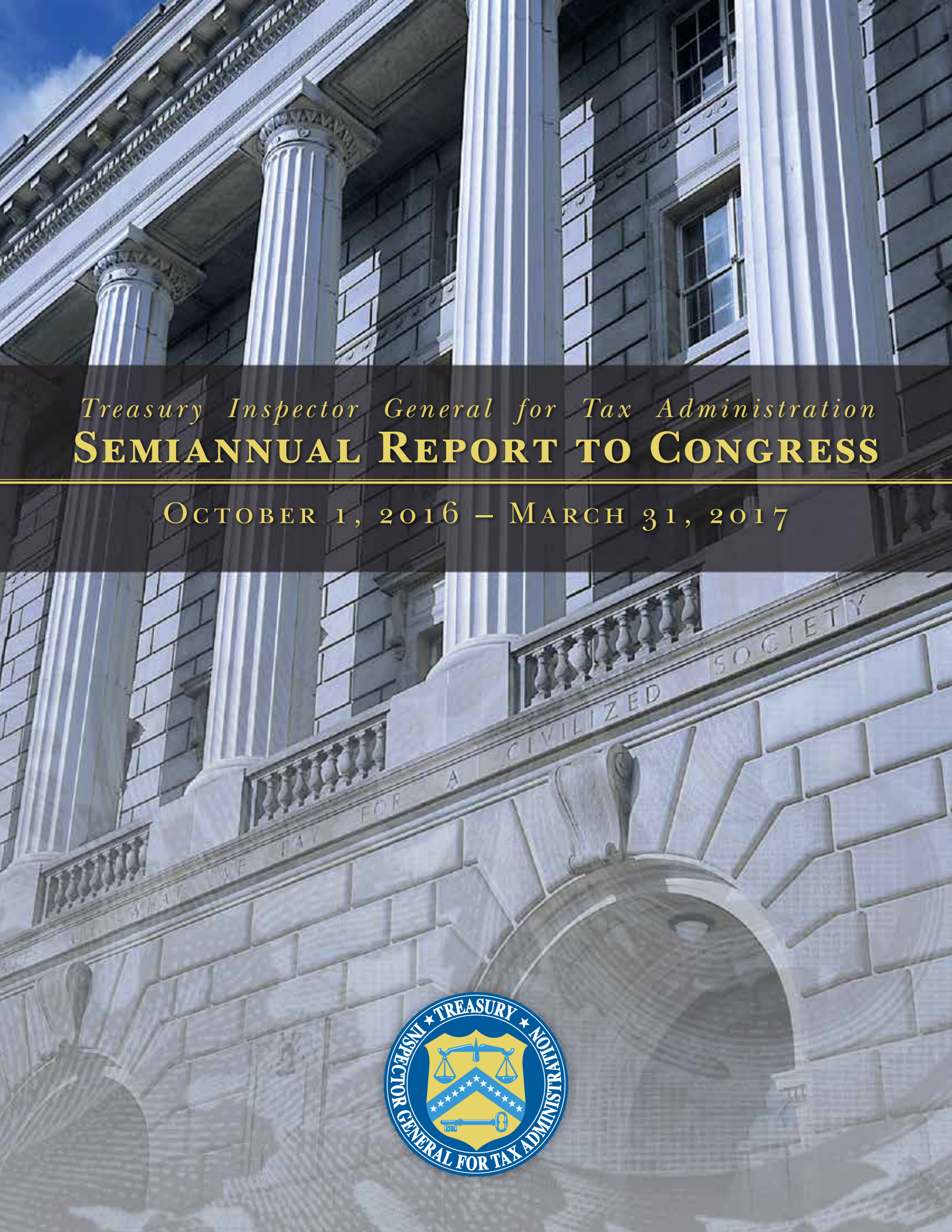


Treasury Inspector General for Tax Administration

Semiannual Report to Congress

October 1, 2016 – March 31, 2017

Treasury Inspector General for Tax Administration (TIGTA)

TIGTA's Vision

Maintain a highly skilled, proactive, and diverse Inspector General organization dedicated to working in a collaborative environment with key stakeholders to foster and promote fair tax administration.

TIGTA's Mission

Provide quality professional audit, investigative, and inspection and evaluation services that promote integrity, economy, and efficiency in the administration of the Nation's tax system.

TIGTA's Core Values

Integrity – Maintain the highest professional standards of integrity, personal responsibility, independence, objectivity, and operational excellence in pursuit of TIGTA's mission.

Organizational Innovation – Model innovative practices in organizational structure, operational programs and processes, audit, investigative, and inspection and evaluation methodologies, and the application of advanced information technology.

Communication – Achieve effective organizational approaches and solutions by encouraging open, honest, and respectful communication among TIGTA's executives, employees, offices, and functions, as well as between TIGTA and its external stakeholders.

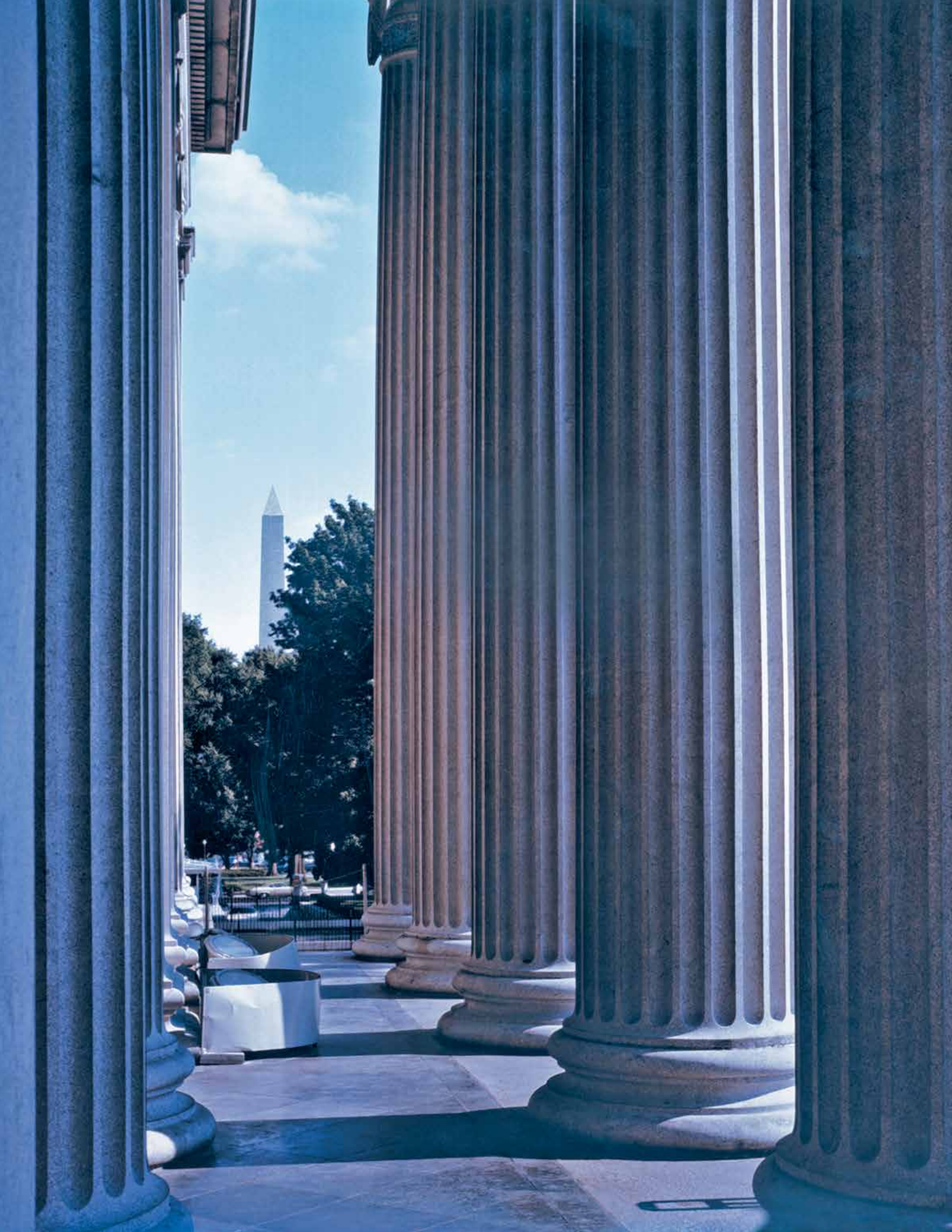
Value Employees – Respect the dignity, contributions, and work-life balance of our employees, and recognize diversity as fundamental to the strength of our organization.

Commitment to Collaboration – Establish and maintain collaborative and professional relationships with other Government and non-Government stakeholders.

Treasury Inspector General for Tax Administration

Semiannual Report to Congress

October 1, 2016 – March 31, 2017



Inspector General's Message to Congress

It is my honor to submit this Semiannual Report to Congress, summarizing the accomplishments of the Treasury Inspector General for Tax Administration (TIGTA) for the period October 1, 2016 to March 31, 2017. This report highlights some of the most notable audits, investigations, and inspections and evaluations performed by TIGTA during this six-month reporting period, as we continue to work diligently in the pursuit of our mission to provide oversight of the Internal Revenue Service (IRS) and to protect the integrity of the Federal system of tax administration.

During this reporting period, TIGTA's Office of Audit has completed 26 audits, and its Office of Investigations has completed 1,393 investigations. In addition, TIGTA's combined audit and investigative efforts have resulted in the recovery, protection, and identification of monetary benefits totaling nearly $169 million ($168.85 million).

Since 2014, we have been reporting on our efforts to combat the largest and most pervasive IRS impersonation scam in the history of this agency. This scam, which continues to rank near the top of the IRS's "Dirty Dozen" tax scams, involves criminals impersonating employees of the IRS or the Department of the Treasury and demanding that taxpayers send them money, usually by wire transfer or prepaid debit cards, or else face immediate jail, deportation, loss of driver's license, or other dire consequences. During this reporting period, TIGTA, in cooperation with other Federal law enforcement agencies, struck a major blow against these scam artists. On October 27, 2016, after an exhaustive three-year TIGTA investigation, the U.S. Department of Justice unsealed an indictment in the Southern District of Texas that charged 56 individuals located primarily in the United States and India, together with five call centers located in India, with multiple criminal charges associated with this massive scam.

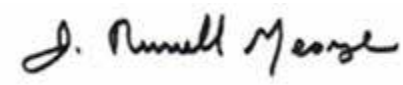
I am pleased to report here that, thanks to these efforts, we have significantly reduced the impact of this scourge. While at its peak, the scammers were claiming more than 500 victims a week, lately the number of weekly victims has dwindled to 30 or less–a mere trickle by comparison. Even so, as of March 31, 2017, more than 10,300 taxpayers have lost in excess of $55 million as victims of this scam. We remain determined to be as aggressive and relentless as these criminals in our commitment to bringing everyone involved in this fraud to justice.

Another type of fraud scheme that is not new but that has been afflicting taxpayers with increasing frequency in recent years is the so-called "lottery scam," in which callers representing themselves as IRS employees contact taxpayers who may be particularly susceptible to scams or fraudulent schemes, such as the elderly or retirement-age people. Two investigative reports included in these pages describe successful investigations conducted by TIGTA against criminals involved in this type of scam.

TIGTA's audit work during the reporting period examined, among other important issues, the IRS's progress in addressing two of the most important challenges that it is currently confronting: the detection and prevention of identity theft and the ongoing need to protect and secure taxpayer information and IRS data resources. We also continued our reporting on our oversight of the IRS's progress in implementing the Affordable Care Act and other recent tax law changes.

We here at TIGTA understand that this Nation's tax system is grounded in voluntary reporting and compliance by its citizens, and that the system can only function efficiently if taxpayers have trust and confidence in its fair and impartial administration. We will continue working tirelessly with Congress, the Administration, the IRS, and other stakeholders in the pursuit of our efforts to promote integrity, economy, and efficiency in the administration of Federal tax laws and regulations.

Sincerely,



J. Russell George
Inspector General

Table of Contents

TIGTA's Profile

The Treasury Inspector General for Tax Administration (TIGTA) provides independent oversight of matters of the Department of the Treasury (Treasury Department or Department) involving activities of the Internal Revenue Service (IRS), the IRS Oversight Board, and the IRS Office of Chief Counsel. Although TIGTA is placed organizationally within the Treasury Department and reports to the Secretary of the Treasury and to Congress, it functions independently from all other offices and bureaus within the Department.

TIGTA oversees all aspects of activity related to the Federal tax system as administered by the IRS. TIGTA protects the public's confidence in the tax system by identifying and recommending strategies for addressing the IRS's management challenges and implementing the priorities of the Treasury Department.

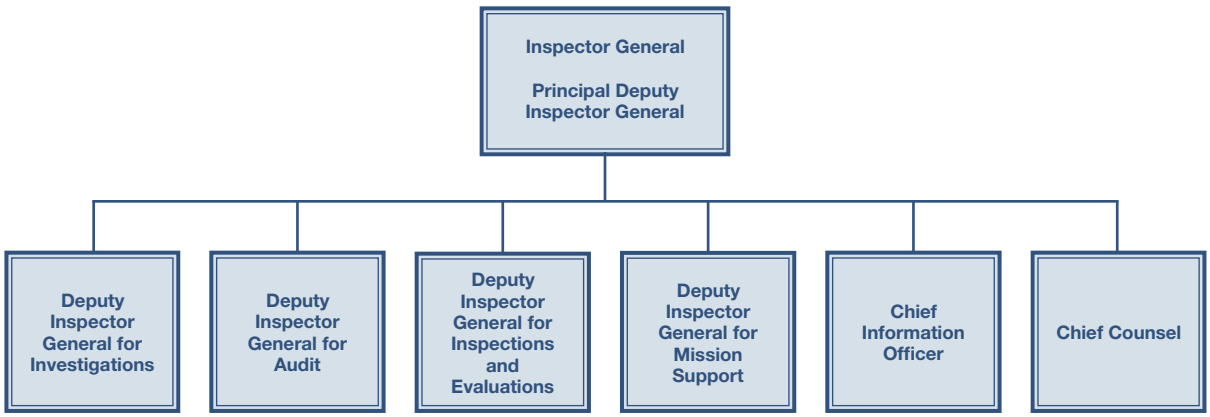
TIGTA's organizational structure is comprised of the Office of the Inspector General and six functional offices: the Office of Investigations; the Office of Audit; the Office of Inspections and Evaluations; the Office of Mission Support; the Office of Information Technology; and the Office of Chief Counsel (see chart on page 6).

TIGTA provides audit, investigative, and inspection and evaluation services that promote economy, efficiency, and integrity in the administration of the Internal Revenue laws.

Statutory Mandate

- **Protect** against IRS employee improprieties and external attempts to corrupt or threaten IRS employees.
- **Provide** policy direction and conduct, supervise, and coordinate audits and investigations related to IRS programs and operations.
- **Review** existing and proposed legislation and regulations related to IRS programs and operations, and make recommendations concerning the impact of such legislation or regulations.
- **Promote** economy and efficiency in the administration of tax laws.
- **Prevent** and detect waste, fraud, and abuse in IRS programs and operations.
- **Inform** the Secretary of the Treasury and Congress of problems and deficiencies identified and of the progress made in resolving them.

Organizational Structure



Authorities

TIGTA has all of the authorities granted under the Inspector General Act of 1978, as amended (Inspector General Act). In addition to the standard authorities granted to Inspectors General, TIGTA has access to tax information in the performance of its tax administration responsibilities. TIGTA also reports potential criminal violations directly to the Department of Justice when TIGTA deems that it is appropriate to do so. TIGTA and the Commissioner of Internal Revenue (Commissioner or IRS Commissioner) have established policies and procedures delineating responsibilities to investigate potential criminal offenses under the Internal Revenue laws. In addition, the Internal Revenue Service Restructuring and Reform Act of 1998 (RRA 98) amended the Inspector General Act to give TIGTA the statutory authority to carry firearms, execute search and arrest warrants, serve subpoenas and summonses, and make arrests as set forth in Internal Revenue Code (I.R.C.) Section (§) 7608(b)(2).

TIGTA's Highlights

Examples of High-Profile Cases by the Office of Investigations

Sixty-one Indicted for Their Roles in IRS Impersonation Scam

In October 2016, J. Russell George, Inspector General for TIGTA, announced a major action concerning the IRS telephone fraud scam.[1] Inspector General George called this the "largest single domestic law enforcement action to date involving this scam," adding that "the indictment is the result of countless hours of solid investigative work and excellent cross-governmental collaboration concerning the massive amounts of fraud that individuals have allegedly perpetrated on the American people."[2]

After an exhaustive three-year joint investigation, the U.S. Department of Justice obtained a superseding indictment in the Southern District of Texas on October 19, 2016, charging 56 individuals, some of whom are located within the United States, plus five call centers located in India, with conspiracy to defraud the United States, conspiracy to commit wire fraud, money laundering conspiracy, and false statements in the application for a passport.[3]

According to the court documents, beginning about January 2012 and continuing until about the date of the indictment, the defendants knowingly and intentionally conspired with each other and others to devise a scheme to defraud and obtain money by means of false and fraudulent pretenses. It was the purpose of the conspiracy that the defendants and others unjustly enrich themselves by fraudulently inducing U.S.-based victims to pay alleged fines and fees and by concealing and disguising the proceeds of the conspirators' unlawful activities.[4]

The indictment included five major call centers, all located in Ahmedabad, Gujarat, India. The call centers were an organization or group of organizations that were used in connection with the scheme to defraud U.S. residents by misleading them into sending money in connection with a number of different scams. One of the scams involved the impersonation of IRS officers and defrauded U.S. residents by misleading them into believing that they owed money to the IRS and would be arrested or fined if they did not pay the alleged back taxes immediately. Another scam involved the impersonation of U.S. Citizen and Immigration Services (USCIS)

---

1 TIGTA Press Release dated Oct. 27, 2016.

2 TIGTA press release dated Oct. 27, 2016.

3 S.D. Tex. Crim. Docket filed Aug. 31, 2016; S.D. Tex. Superseding Indict. filed Oct. 19, 2016.

4 S.D. Tex. Superseding Indict. filed Oct. 19, 2016.

officers, and defrauded U.S. residents by misleading them into believing that they would be deported unless they immediately paid a fine for alleged problems with their USCIS paperwork.[5]

The conspirators held one or more roles in furtherance of the conspiracy. According to the indictment, "Call Center Operators" were located in India and managed the day-to-day operations of the call centers. "Callers" made the fraudulent and extortionate calls to victims in the United States and elsewhere pretending to be U.S. Government officials or money lenders. "Runners" located in the United States retrieved cash payments of scammed funds via money transmitters.[6] "Domestic Managers" were also located in the United States and directed the runners' activities and sometimes provided resources such as vehicles and credit cards for travel.[7]

As part of the conspiracy, conspirators operating at call centers located primarily in India obtained and distributed lead lists and scripts containing Personally Identifiable Information (PII) for the purpose of contacting and defrauding potential victims. The callers, pretending to be U.S. Government officials or lenders, at times used "spoofed"[8] numbers to make the calls appear to originate from a Federal agency and telephoned U.S. victims to threaten them with prosecution, arrest, or other adverse actions for purported tax or immigration violations unless they paid the alleged fines or fees. Callers instructed victims to go immediately to banks to withdraw money to purchase prepaid stored-value cards[9] from retail stores and provide them with the unique serial numbers of the cards.[10]

The U.S.-based defendants obtained general purpose reloadable (GPR) cards, which could be used like debit cards without being associated with a personal bank account. The cards were activated by registering them using misappropriated PII. The defendants transferred victim funds from stored-value cards to the GPR cards, used the GPR cards loaded with scammed funds to purchase money orders, and then

---

5 Id.

6 A business that helps a person to send or receive money within the United States or abroad, typically by means of a wire transfer, money order, or stored-value card. Money transmitters must have a license to operate and are regulated by the Office of the Commissioner of Banks.

7 S.D. Tex. Superseding Indict. filed Oct. 19, 2016.

8 A mechanism whereby callers deliberately falsify the information transmitted to a victim's caller ID and thereby disguise their identity or location.

9 A card that can have monetary value placed onto it by a purchaser and can be used to fund general purpose reloadable (GPR) cards.

10 S.D. Tex. Superseding Indict. filed Oct. 19, 2016.

deposited the money orders into the U.S. bank accounts of various individuals and businesses.[11]

The callers extorted one victim, a resident of California, of approximately $136,000 by fraudulently pretending to be IRS agents and demanding payment for alleged tax violations. The victim was directed to purchase 276 MoneyPak® stored-value cards with a total value of approximately $136,000 and to transmit the Personal Identification Numbers (PIN) associated with the stored-value cards to the callers, after which the conspirators transferred the scammed funds to GPR cards. One defendant, who was an information technology contractor for a private New York company, then used stolen PII from the company's database to activate GPR cards loaded with funds scammed from the victim.[12]

The callers extorted another victim, from Brooklyn, New York, of $121,166 by fraudulently purporting to be IRS employees, threatening to arrest the victim, and demanding payment for alleged tax violations. The callers then directed the victim to make payments into approximately 20 different bank accounts and to send wire transfers via Western Union®.[13]

This complex fraud scheme resulted in hundreds of millions of dollars in victim losses. Over 15,000 known victims have incurred losses attributable to scam calls, and upwards of 50,000 individuals have had their identities misappropriated based on the unauthorized use of their PII to register GPR cards.[14]

As of the end of this reporting period, more than 1.9 million people have reported to TIGTA that they received an impersonation call. Inspector General George has said that the work of TIGTA's Office of Investigations is a shining example of what an agency can do when it dedicates itself to focusing on even the most tangled and complicated of criminal schemes and that TIGTA will continue to pursue investigations into this type of criminal activity until it brings those involved to justice.[15]

A number of defendants have been arrested in various locations within the United States,[16] and additional legal actions are anticipated.

---

11 S.D. Tex. Superseding Indict. filed Oct. 19, 2016.

12 Id.

13 Id.

14 Id.

15 TIGTA press release dated Oct. 27, 2016.

16 S.D. Tex. Crim. Docket filed Aug. 31, 2016.

Pennsylvania Man Sentenced to Eight Years in Prison in Fraud Scheme

On February 15, 2017, in the Eastern District of Pennsylvania, Steven Hameed was convicted of and sentenced for conspiracy, corrupt interference with the Internal Revenue laws, fictitious obligations, conversion of Government property, and bank fraud.[17] Hameed and his coconspirators, Darnell Young and Damond Palmer, were indicted for the offenses in December 2015.[18] Young was convicted of the offenses on October 19, 2016, and Palmer was convicted of conspiracy and bank fraud on October 19, 2016.[19]

According to the court documents, Hameed, Young, and Palmer were self-proclaimed members of a group of individuals who held themselves out as "sovereign" citizens. Hameed and Young purported to be a married couple, but were not legally married in the Commonwealth of Pennsylvania. The indictment charged that from about February 2010 until March 2013, Hameed, Young, and Palmer conspired together and with others to knowingly execute a scheme to convert property of the U.S. Department of Housing and Urban Development (HUD), to devise a scheme to obtain bank-owned property, and to obstruct and impede the due administration of the IRS.[20]

As part of their scheme, the conspirators created false and fraudulent deeds purporting to convey ownership of properties to Hameed, Young, Palmer, or others and filed these false deeds with the Delaware County Recorder of Deeds. They did so in an attempt to obtain ownership and control over properties that were not legally owned by the conspirators in order to occupy, rent, and/or sell such properties for their own financial profit.[21]

Specifically, the indictment charged that Hameed, Young, and Palmer caused to be delivered to the Delaware County Government Center in Media, Pennsylvania, false and fraudulent deeds for 54 properties over which they attempted to assert ownership for their own personal gain. These properties were, in fact, owned by banks, HUD, and private citizens or businesses. After filing, or attempting to file, the false deeds, the conspirators attempted to convert the properties to their own use, falsely asserting ownership either by occupying the houses themselves or by attempting to rent or sell the properties.[22]

---

17 E.D. Pa. Judgment filed Feb. 17, 2017.

18 E.D. Pa. Indict. filed Dec. 1, 2015.

19 E.D. Pa. Judgment filed Oct. 21, 2016; E.D. Pa. Judgment filed Oct. 20, 2016.

20 E.D. Pa. Indict. filed Dec. 1, 2015.

21 Id.

22 Id.

Also, the indictment charged that, with intent to defraud, Hameed and Young presented a false and fictitious document appearing to be an actual security or financial instrument issued under the alleged authority of the Treasury Department to purchase a property in Chester, Pennsylvania.[23]

According to the indictment, Hameed, Young, and Palmer knowingly, willfully, and unlawfully conspired to corruptly obstruct and impede the IRS by filing false tax forms intended to intimidate and harass Government officials and law enforcement based upon the submission of false forms to the IRS.[24]

The indictment charged that the defendants filed IRS Forms 1099-DIV, *Dividends and Distributions*, and Forms 1099-INT, *Interest Income*, falsely stating that one of them had paid money, representing either dividends or interest, to the individual that the form named as the payee. They did so in an attempt to cause IRS scrutiny of the payee when the payee did not report the fabricated income to the IRS, knowing that no dividend or interest income had been paid to the individuals listed on the false forms. A total of 273 forms were filed, and most stated an income amount of $9,999,999.[25]

Hameed also filed a frivolous lawsuit in U.S. District Court for the District of Columbia against 15 Delaware County judges and law enforcement individuals, in a further attempt to harass and intimidate those individuals.[26]

Hameed was sentenced to 96 months' imprisonment, followed by five years of supervised release.[27] Young and Palmer were sentenced in October 2016 to 40 months in prison for Young and one day in prison for Palmer, followed by five years of supervised release each.[28] The three collectively are required to pay a total restitution in the amount of $190,818.84. Hameed was further ordered not to file any frivolous lawsuits or to prepare and/or file any false financial documents, tax documents, and/or liens.[29]

---

23 Id.

24 Id.

25 Id.

26 E.D. Pa. Indict. filed Dec. 1, 2015.

27 E.D. Pa. Judgment filed Feb. 17, 2017.

28 E.D. Pa. Judgment filed Oct. 21, 2016; E.D. Pa. Judgment filed Oct. 20, 2016.

29 E.D. Pa. Judgment filed Feb. 17, 2017.

Example of High-Profile Reports by the Office of Audit

Efforts Continue to Result in Improved Identification of Fraudulent Tax Returns Involving Identity Theft; However, Accuracy of Measures Needs Improvement

Recognizing the impact that identity theft has on tax administration, the IRS continues to adopt strategies to improve detection and prevention. While these strategies have led to many notable improvements, identity theft continues to evolve and become more sophisticated. As a result, the IRS began to explore other initiatives that would assist with its overall detection and prevention efforts, such as convening a Security Summit and coding Forms W-2, *Wage and Tax Statement*. The IRS's Identity Theft Taxonomy measures its efforts to defend against identity theft and to identify areas requiring additional effort.

This audit assessed the effectiveness of the IRS's continued efforts to detect and prevent identity theft, measure undetected identity theft, and coordinate identity-theft information with other Government agencies and tax industry partners.

TIGTA identified continued reductions in the volume of undetected potentially fraudulent tax returns. TIGTA's review of Tax Year (TY) 2013 returns identified 568,329 undetected potentially fraudulent tax returns with claimed tax refunds totaling more than $1.6 billion, which represented a reduction of more than $523 million from the prior year. However, the false reporting of wages and withholding continues to account for the largest amount ($1.3 billion) of undetected potentially fraudulent tax return refunds. With the passage of legislation to accelerate the reporting of Forms W-2,[30] the IRS should be able to significantly reduce the number of these undetected tax returns.

TIGTA also reported that using State lead data during tax return processing can improve identity-theft detection efforts. Finally, TIGTA found that the accuracy of the Identity Theft Taxonomy quantification for both protected and unprotected revenue could be improved. For example, the IRS's estimate of protected revenue was overstated by almost $2.4 billion as a result of the incorrect calculation of refunds associated with rejected electronically filed tax returns.

TIGTA recommended that the IRS:

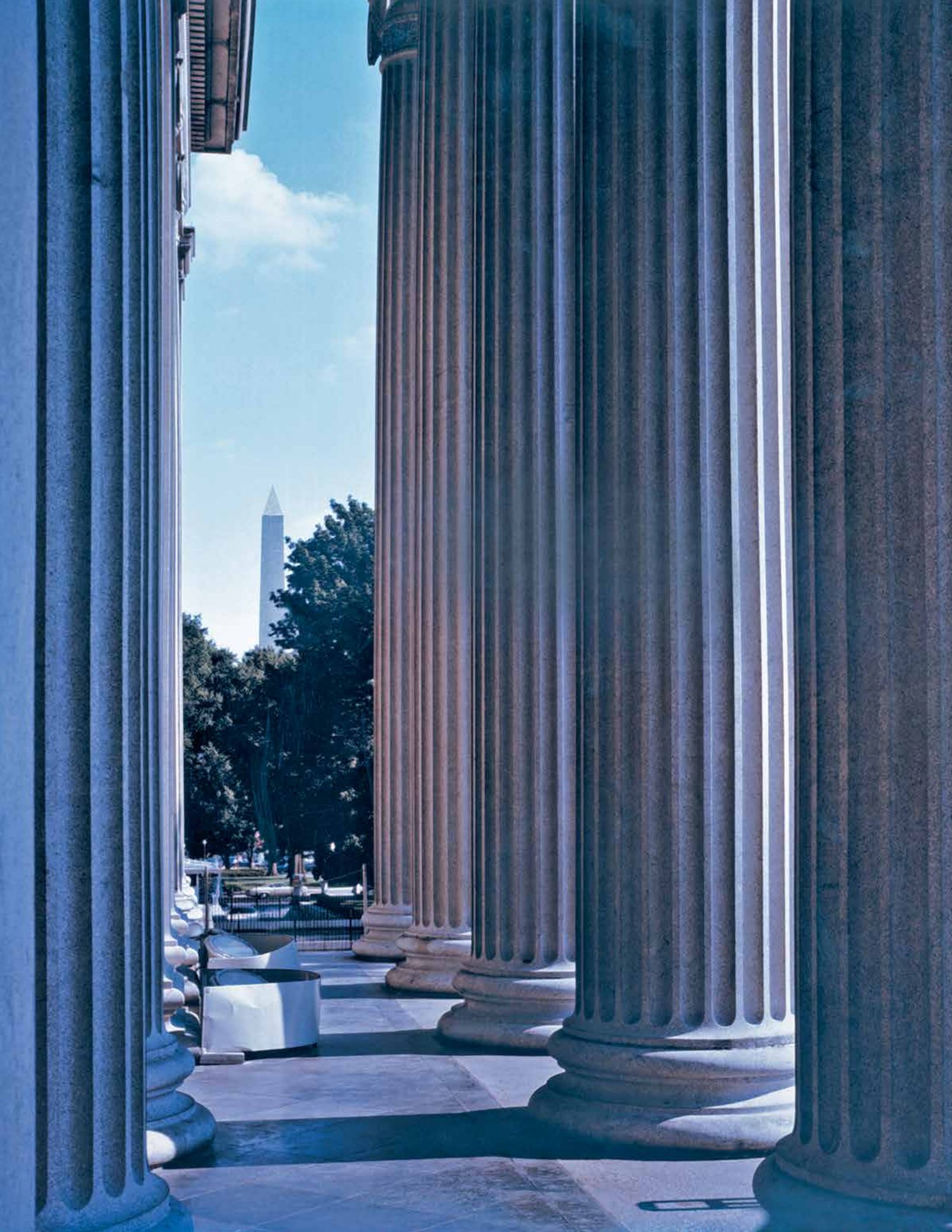
- Expand the use of its identity-theft models to include all accelerated Forms W-2;
- Develop a process to use State lead data; and

---

30 Protecting Americans From Tax Hikes Act of 2015, Pub. L. No. 114-113, § 201(a), 129 Stat. 2242, 3076.

- Update the Identity Theft Taxonomy methodology used to quantify unprotected and protected revenue.

IRS management agreed with all of the recommendations.
Reference No. 2017-40-017



Promote the Economy, Efficiency, and Effectiveness of Tax Administration

TIGTA's Office of Audit strives to promote the economy, efficiency, and effectiveness of tax administration. TIGTA provides recommendations to improve IRS systems and operations and to ensure the fair and equitable treatment of taxpayers. TIGTA's comprehensive and independent performance and financial audits of the IRS's programs and operations primarily address statutorily mandated reviews and high-risk challenges for the IRS.

The IRS's implementation of audit recommendations results in:

- Cost savings;
- Increased or protected revenue;
- Protection of taxpayers' rights and entitlements; and
- More efficient use of resources.

Each year, TIGTA identifies and addresses the IRS's major management and performance challenges. The Office of Audit places audit emphasis on statutory coverage required by RRA 98 and other laws, as well as areas of concern to Congress, the Secretary of the Treasury, the Commissioner of the IRS, and other key stakeholders.

Audit Emphasis Areas for October 2016 Through March 2017

- Security Over Taxpayer Data and Protection of IRS Resources
- Implementing the Affordable Care Act and Other Tax Law Changes
- Improving Tax Compliance
- Providing Quality Taxpayer Service Operations
- Protecting Taxpayer Rights
- Achieving Program Efficiencies and Cost Savings

The following summaries highlight significant audits completed in each area of emphasis during this six-month reporting period:

Security Over Taxpayer Data and Protection of IRS Resources

As cybersecurity threats against the Federal Government continue to grow, protecting the confidentiality of taxpayer information will continue to be a top concern for the

IRS. The increasing number of data breaches in the private and public sectors means more PII than ever before is available to unscrupulous individuals. Much of the data is detailed enough to circumvent most authentication processes. Therefore, it is critical that the methods that the IRS uses to authenticate individuals' identities promote a high level of confidence that tax information and services are provided only to individuals who are entitled to receive them.

The existence of differing levels of authentication assurance among the various access methods increases the risk of unscrupulous individuals accessing and obtaining personal taxpayer information and/or defrauding the tax system. The IRS has undertaken a number of steps to improve systems and provide for more secure authentication, including strengthening application and network controls. However, additional actions could further improve security over the authentication process.

Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners

The IRS shares data with various outside entities, including Federal, State, and local agencies; financial institutions; and contractors for tax administration purposes. The data may include sensitive information, such as PII and other taxpayer information. IRS and Federal guidelines require that sensitive data be protected during transmission to prevent unauthorized access or disclosure.

This audit was initiated to determine whether the IRS is properly protecting the data that it transmits to external entities through secure file transfer technology. The audit also determined whether the IRS was maintaining encryption controls and other security configurations in accordance with the National Institute of Standards and Technology.

The IRS uses three methods to transfer data to external partners: 1) a commercial off-the-shelf product for transfers over the Internet, 2) a commercial off-the-shelf product for direct mainframe-to-mainframe data transfers, and 3) drop boxes to allow the IRS and its external partners to place and retrieve data transfers. In reviewing all three of these external file transfer methods, TIGTA found that the IRS did not ensure that encryption requirements are being enforced and that only secure protocols are being used in order to fully protect information during transmission.

TIGTA also found that the IRS did not remediate high-risk vulnerabilities or install security patches on file transfer servers in a timely manner. For example, TIGTA found 61 servers with high-risk vulnerabilities, 10 servers with outdated versions of Microsoft Windows and UNIX operating systems still in operation, and 32 servers missing 18 unique security patches, of which four were deemed critical.

Lastly, the IRS did not ensure that corrective action plans for correcting security control weaknesses, including some of the weaknesses previously mentioned, met IRS standards. This reduced the assurance that the weaknesses would be corrected timely.

TIGTA recommended that the IRS:

- Enforce IRS policy to encrypt all data transmissions from end to end, using Federally compliant encryption or, if external partners cannot use Federally compliant encryption, ensure that risk-based decisions have been properly approved and data transmissions have been properly authorized;
- Ensure that file transfer components are properly configured, patching is timely, and outdated operating systems are replaced;
- Centralize and consolidate the IRS's external transfer environment to the extent possible, using a managed file transfer solution that supports end-to-end Federally compliant encryption to maximize security and efficiency; and
- Ensure that remediation plans are effective for correcting weaknesses in a timely manner.

IRS management agreed to ensure that data transmissions are properly authorized and remediation plans for correcting weaknesses are effective. It partially agreed to end-to-end encryption enforcement, proper configurations, patching, and operating systems, indicating that it already had processes in place. IRS management disagreed that it could further consolidate its external file transfer environment, but would reconsider as partner agreements are revalidated. TIGTA believes that the IRS should proactively work with partners to upgrade to end-to-end encryption solutions, rather than waiting, because the data transmitted are highly sensitive.
Reference No. 2017-20-004

Continuity Planning and Emergency Preparedness Follow-Up Audit

Effective continuity planning and emergency preparedness can facilitate the IRS's ability to prepare for, respond to, and recover from emergencies. After an emergency occurs, it is important to timely resume business operations, because an extended disruption to IRS facilities can affect key processes. Processing delays could ultimately have a negative impact on the Nation's economy as well as taxpayer data and compliance.

This audit was initiated to determine: 1) if the IRS had effectively addressed the eight recommendations identified in TIGTA's previous audit on continuity planning, [31] and 2) how the IRS responded to any recent incidents that would require the use of a continuity plan.

The IRS fully implemented four of TIGTA's eight prior recommendations. Specifically, the IRS updated its continuity procedures and improved the management of training and exercises. The IRS updated the manual associated with continuity planning and defined requirements for issuing the annual certification of continuity readiness to the Treasury Department. Previously missing continuity plans were prepared, and all 22 IRS business units maintained current continuity plans on the required repository system. The IRS also issued standard operating procedures for monitoring continuity training. Additionally, in Fiscal Year (FY) 2016, the Senior Commissioner's Representative – Continuity of Operations office–established a process for reviewing and approving each business unit's continuity plan.

However, four prior recommendations were not fully addressed. The IRS required the use of the continuity plan templates, but two business units were still missing required portions of their plans. Although standard operating procedures were issued for monitoring training, all training was not completed timely, and employees who were no longer actively conducting continuity program duties were included in calculations used to monitor the program's effectiveness. TIGTA's review of the tracking of tests and exercises found that 12 percent were completed after the required date and that there were 22 late After-Action Report submissions for FY 2015.

Finally, the IRS reacted quickly to three recent incidents reviewed by TIGTA that disrupted or had the potential to disrupt operations. For all three incidents, the IRS implemented its continuity plans and was able to resume business operations promptly. However, no After-Action Report was completed for one of the three incidents.

TIGTA recommended that the IRS:

- Review business unit continuity plans annually and ensure that they address all required elements;
- Improve monitoring of tests and exercises by requiring timely completion and After-Action Report submissions and ensure that the list of active personnel required to complete mandatory continuity training is updated; and

---

31 TIGTA, Ref. No. 2013-10-102, Improvements Are Needed to Ensure Timely Resumption of Critical Business Processes After an Emergency (Sept. 2016).

- Ensure that After-Action Reports are prepared for all real incidents, so that deficiencies are tracked and monitored.

IRS management agreed with all of the recommendations.
Reference No. 2017-10-020

Implementing the Affordable Care Act and Other Tax Law Changes

The IRS was challenged during the 2016 Filing Season by the passage of legislation that extended a number of expired tax provisions.[32] For example, the Trade Preferences Extension Act of 2015[33] impacts the 2016 Filing Season and prohibits individuals that claim the foreign earned income exclusion or housing deduction from receiving the refundable Additional Child Tax Credit (ACTC). This Act also retroactively extends the Health Coverage Tax Credit (HCTC) for TY 2014 and continues the credit through TY 2019.[34] Further, the Protecting Americans From Tax Hikes Act of 2015[35] (PATH Act) includes program integrity provisions specifically intended to reduce fraudulent and improper payments related to the Earned Income Tax Credit, the Child Tax Credit (CTC), the ACTC, and the American Opportunity Tax Credit (AOTC). These integrity provisions expand the IRS's ability to verify earned income before claims are paid, increase tax return preparer due-diligence requirements and taxpayer reporting requirements, and expand the IRS's ability to ban individuals previously determined to have filed reckless or fraudulent CTC and AOTC claims from receiving the credit. The majority of these program integrity provisions were effective January 1, 2017.

To reduce the impact on the filing season, the IRS monitored the status of the pending legislation and took steps to implement the extension of these provisions prior to their enactment. These efforts enabled the IRS to begin accepting and processing individual tax returns on January 19, 2016, as scheduled.

Results of the 2016 Filing Season

The filing season, defined as the period from January 1 through mid-April, is critical for the IRS because it is during this time that most individuals file their income tax returns and contact the IRS if they have questions about specific laws or filing procedures. TIGTA conducted this review to evaluate whether the IRS timely and

---

32 TIGTA, Ref. No. 2016-40-034, Interim Results of the 2016 Filing Season (Mar. 2016).

33 Pub. L. No. 114-27, 129 Stat. 362.

34 The HCTC originally expired at the end of Calendar Year 2013.

35 Pub. L. No. 114-113, 129 Stat. 2242, 3041-3129.

accurately processed individual paper and electronically filed tax returns during the 2016 Filing Season.

TIGTA's review confirmed that the IRS accurately updated tax publications, forms, and information found on the IRS website and accurately processed individual tax returns involving the implementation of key extender tax provisions. However, TIGTA found that the IRS did not establish adequate processes to ensure that documentation required to support HCTC claims was associated and reviewed before processing claims and allowing the credits. The review also found that employee errors resulting from the manual processing of these claims further delayed some taxpayer refunds. For example, TIGTA's review of 6,300 electronically filed tax returns and 356 paper tax returns that had been processed as of April 28, 2016, with HCTC claims totaling more than $20.8 million, identified 450 returns (6.8 percent) that contained a processing error.

Additionally, the IRS has not implemented computer programming changes to correct Residential Energy Efficient Property Credit processing errors that TIGTA identified during the 2015 Filing Season. As a result, the IRS incorrectly limited the Residential Energy Efficient Property Credit on 731 tax returns processed as of April 28, 2016, which caused these taxpayers to receive approximately $1.2 million less in credits than they were entitled to receive.

TIGTA also found that computer programming errors are still causing some direct deposits not to convert to a paper check, as required. TIGTA's analysis of the 86 million deposit requests identified 5,605 deposit attempts, totaling approximately $9.2 million, that did not convert to a paper check as required.

Furthermore, the number of taxpayers whom the IRS assists at Taxpayer Assistance Centers (TAC) continues to decrease. The IRS assisted 5.6 million taxpayers in FY 2015, but only 4.5 million taxpayers in FY 2016, a 20 percent decrease. Finally, as of May 7, 2016, the IRS reported that assistors answered 14.1 million calls and provided a 69 percent Level of Service with a 12.2-minute average wait time in FY 2016. The Level of Service for the 2015 Filing Season was 37.7 percent.

As a result, TIGTA made several recommendations, including that the IRS review incorrectly processed HCTC and Residential Energy Efficient Property Credit claims identified by TIGTA, and that it implement necessary computer programming changes related to the Residential Energy Efficient Property Credit.

IRS management agreed with all of the recommendations.
Reference No. 2017-40-014

Improving Tax Compliance

PII is a specific type of sensitive information that may include tax returns and return information. Laws require that the IRS protect PII, tax returns, and return information for different reasons, most notably the protection of privacy. Moreover, the loss, theft, or unauthorized disclosure of taxpayer PII or tax return information places individuals at serious risk of identity theft. Additionally, the proper protection of such information helps maintain taxpayer confidence and the IRS's reputation for privacy protection, which are critical for the IRS to perform its mission.

Employees Sometimes Did Not Adhere to E-Mail Policies, Which Increased the Risk of Improper Disclosure of Taxpayer Information

This audit was initiated because e-mail is a prevalent form of communication at the IRS. Employees who have frequent contact with taxpayers, *e.g.*, revenue officers and revenue agents, need to ensure that appropriate steps are being taken to safeguard e-mails. The audit determined whether the IRS's Small Business/Self-Employed (SB/SE) Division employees were following e-mail policies and properly safeguarding taxpayer PII and tax return information contained in e-mail correspondence.

TIGTA reviewed a random sample of 80 SB/SE Division employees' e-mails sent during four weeks in May and June 2015 and determined that 39 employees (49 percent) sent a total of 326 unencrypted e-mails. Those unencrypted e-mails contained the PII or tax return information of 8,031 different taxpayers that had been sent internally to other IRS employees or externally to non-IRS e-mail accounts. However, the majority of these unencrypted e-mails (275 of the 326) had been sent internally to other IRS employees, and e-mails sent inside the IRS internal information system's firewall pose less risk of improper disclosure or improper access than do external e-mails. TIGTA also identified 51 unencrypted e-mails containing taxpayer PII or tax return information that were sent externally to non-IRS e-mail accounts. These employees failed to follow Internal Revenue Manual (IRM) requirements and risked exposing the information to unauthorized persons.

Additionally, 20 e-mails sent by six employees to personal e-mail accounts involved official IRS business. SB/SE Division employees may not be aware of the restriction on using personal e-mail because the IRM's *Standards for Using Email* do not include this restriction.

The IRS Enterprise e-Fax (EEFax) capability was implemented in early 2013 without encryption capability. TIGTA identified 193 unencrypted e-mails containing taxpayer PII or tax return information that were routed to the EEFax servers via the e-mail

system. Because the EEFax does not use encryption, its use could result in the interception and disclosure of taxpayer PII or tax return information.

TIGTA recommended that the IRS:

- Consider the feasibility of a systemic solution to ensure that taxpayer PII and tax return information is encrypted and, until such time, consider requiring the default Outlook setting for certain employees to encrypt sent e-mail messages;
- Ensure that managers are aware of e-mail violations and take appropriate disciplinary action;
- Update the IRM to prohibit IRS employees from using a personal e-mail account to conduct official business of the Government; and
- Request an information technology update to allow encrypted messages to be sent to the EEFax server.

IRS management agreed with all of the recommendations.
Reference No. 2017-30-010

Providing Quality Taxpayer Service Operations

Tax-related identity theft continues to be one of the biggest challenges facing the IRS. To provide relief to identity-theft victims, the IRS began issuing Identity Protection Personal Identification Numbers (IP PIN) to eligible taxpayers in FY 2011. An IP PIN is a six-digit number assigned to taxpayers that allows their tax returns/refunds to be processed without delay and helps prevent the misuse of their Social Security Numbers (SSN) to file fraudulent Federal income tax returns. For Processing Year (PY)[36] 2016, the IRS issued more than 2.7 million IP PINs to taxpayers for use in filing their tax returns.

Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers

The IRS did not deactivate the online IP PIN application after a security breach was identified on May 17, 2015. Instead, it implemented risk mitigation processes. TIGTA made repeated recommendations to shut down the application until a stronger level of online authentication could be implemented and advised the IRS that its risk mitigation processes were not always working as intended.

---

36 The calendar year in which the tax return or document is processed by the IRS.

This audit was initiated to assess the IRS's actions to improve and expand the IP PIN Program. This included assessing corrective actions to TIGTA's prior recommendations[37] and the IRS's decision to not deactivate the online IP PIN application after security weaknesses were identified.

TIGTA's review of 32,623 tax returns filed between January 19 and May 24, 2016, with an IP PIN that was viewed online, identified12,020 returns (36.8 percent) that were not manually reviewed as required. In addition, taxpayer accounts were not always consistently updated to ensure that IP PINs were generated for taxpayers as required. The IRS failed to generate an IP PIN for approximately 2 million taxpayers for whom the IRS resolved an identity-theft case confirming that the taxpayer was a victim.

Also, the IP PIN notice continues to contain inaccurate information. The IRS mailed approximately 2.7 million IP PIN notices to taxpayers for PY 2016, erroneously instructing them not to use their IP PIN if they are claimed as a dependent on a tax return.

Finally, the IRS's Opt-In Program was designed to focus on taxpayers in locations with the highest per capita rate of identity theft and offer them the opportunity to obtain an IP PIN before becoming a victim of tax-related identity theft. However, the IRS has not updated its identification of locations that may now have the highest per capita rates based on identity-theft complaints. In addition, taxpayers in Opt-In Program locations may be unaware of the option to obtain an IP PIN.

TIGTA recommended that the IRS ensure that:

- An authentication risk assessment is completed and documented subsequent to all future system security breaches to an online application;
- All functions have consistent procedures for adding identity-theft markers that create an IP PIN;
- Accurate information is provided to taxpayers on IRS notices;
- Processes are developed to identify taxpayers in locations with the highest per capita rates of identity theft; and
- An outreach strategy is developed to increase taxpayer awareness of the Opt-In Program.

---

37 TIGTA Ref. No. 2014-40-086, Identity Protection Personal Identification Numbers Are Not Provided to All Eligible Taxpayers (Sept. 2014); TIGTA Ref. No. 2016-40-007, Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed (Nov. 2015).

IRS management agreed with four recommendations, but did not agree that processes need to be developed to identify taxpayers in locations with the highest per capita rates of identity theft. TIGTA stated that this decision is contrary to the intent of the Opt-In Program, which is to focus on taxpayers in States and locations with the highest per capita rates of identity theft.
Reference No. 2017-40-026

Protecting Taxpayer Rights

The Currency and Foreign Transactions Reporting Act of 1970,[38] also referred to as the Bank Secrecy Act, requires U.S. financial institutions to file reports of currency transactions exceeding $10,000. Section 5324(a) of the Bank Secrecy Act states that no person shall, for the purpose of evading the reporting requirements, cause or attempt to cause a U.S. financial institution to fail to file a report required or structure.[39] Whoever violates the structuring law can be fined, imprisoned, or both. Any property involved in violation of this law may be seized and forfeited.

Criminal Investigation Enforced Structuring Laws Primarily Against Legal Source Funds and Compromised the Rights of Some Individuals and Businesses

In October 2014, a new policy was instituted by IRS Criminal Investigation (CI) that it would no longer pursue the seizure and forfeiture of funds related to legal source structuring. In the same month that the policy changed, the *New York Times* reported that CI had been seizing funds in structuring investigations without filing a criminal complaint. Property owners were left to prove their innocence, and many gave up trying.[40] This audit was initiated to evaluate the IRS's use of seizures against property owners suspected of structuring transactions to avoid Bank Secrecy Act reporting requirements.

TIGTA found that most of the seizures for structuring violations involved legal source funds from businesses. While current law does not require that the funds

---

38 31 United States Code (U.S.C.) § 5311 et seq.

39 A person structures a transaction if that person, acting alone or in conjunction with or on behalf of other persons, conducts or attempts to conduct one or more transactions in currency in any amount, at one or more U.S. financial institutions, on one or more days, in any manner, for the purpose of evading the Currency Transaction Report filing requirements. This includes, but is not limited to, breaking down a single currency sum exceeding $10,000 into smaller amounts that may be conducted as a series of transactions at or less than $10,000.

40 Shaila Dewan, Law Lets I.R.S. Seize Accounts on Suspicion, No Crime Required, N.Y. Times, Oct. 25, 2014, at A1.

have an illegal source (*e.g.*, money laundering or criminal activity other than alleged structuring), the purpose of CI's civil forfeiture program is to interdict criminal enterprises. As a result, $17.1 million was seized and forfeited to the Government in 231 legal source cases. CI primarily relied on patterns of banking transactions to establish probable cause to seize assets for structuring violations.

In most instances, interviews with the property owners were conducted after the seizure, to determine the reason for the pattern of banking transactions and whether the property owner had knowledge of the banking law and had intent to structure. CI procedures required agents to give subjects advice of rights in I.R.C. cases but not in Bank Secrecy Act cases. Noncustodial statements of rights, such as the right to remain silent, were provided in only five of the 229 interviews conducted. For 54 investigations, the property owners provided realistic defenses or explanations, and for 43 of those cases, there was no evidence that CI considered those defenses or explanations. During 202 interviews, the property owners were not adequately informed of important information, such as the purpose of the interview. The outcomes for legal source cases lacked consistency. In 37 investigations, the Government appeared to have bargained nonprosecution to resolve the civil case.

CI also needs to improve its process for identifying grand jury information.

TIGTA made nine recommendations, including that the IRS:

- Establish controls to ensure that CI is selecting cases that meet the IRS's goals and policies;
- Return funds forfeited from legal source cases with no illegal activity;
- Ensure that reasonable explanations are considered when interviews are conducted;
- Ensure appropriate referrals to the IRS's Examination function; and
- Improve the process for designating grand jury information.

IRS management agreed with five of the nine recommendations and partially agreed with another. It disagreed with the recommendation that the IRS establish guidance on bargaining nonprosecution and that it adopt procedures that strive for fair and consistent outcomes, and it did not agree to improve the IRS's grand jury information designation process.
Reference No. 2017-30-025

Achieving Program Efficiencies and Cost Savings

Federal law and policy both require agencies, including the IRS, to charge a user fee to recover the cost of providing certain services to the public that confer a special benefit to the recipient. The price of user fees for requests processed by the IRS's Office of Chief Counsel (Chief Counsel) ranges from $150 to more than $28,000, depending on the type of request. It is important to the taxpayer that fees for these requests are processed accurately and refunded when required.

The Office of Chief Counsel Accurately Administered User Fees but Could Improve Its User Fee Refund Process

This audit was initiated to determine whether Chief Counsel accurately and efficiently administers user fees. TIGTA found that Chief Counsel accurately administered fees for requests for rulings by assigning the correct user fee case type and assessing the appropriate fee–including reduced user fees when applicable. In FY 2015, it accurately processed 3,530 user fee collections valued at more than $20 million.

There are areas in which Chief Counsel could improve its process. Specifically, in FY 2015 Chief Counsel took an average of five business days to deposit user fee receipts, which exceeds the statutory requirement to deposit payments within three days. In order to comply with Federal requirements and have timely access to funds, Chief Counsel should deposit user fee payments within three days of receipt. Additionally, TIGTA identified differences between information contained in Chief Counsel's paper case files and its electronic data.

Finally, although cases were initially processed accurately, Chief Counsel's process does not ensure that user fee refunds for overpayments, or for payment on requests for which Chief Counsel declined to rule, are processed for remittance back to taxpayers. Specifically, TIGTA found 24 user fee overpayments totaling almost $58,000 that were not refunded in FY 2015.

TIGTA made several recommendations, including that Chief Counsel should make user fee deposits within three days of receipt; provide training to employees to ensure that proper dates are entered into its case management information system; implement policies to process refunds; and issue refunds to the 24 taxpayers that overpaid user fees in FY 2015 without receiving a refund.

IRS management agreed with all of TIGTA's recommendations.
Reference No. 2017-10-012

Protect the Integrity of Tax Administration

TIGTA is statutorily mandated to protect the integrity of Federal tax administration. TIGTA accomplishes its mission through the investigative work conducted by the Office of Investigations (OI). Through its investigative programs, OI protects the integrity of the IRS and its ability to collect revenue owed to the Federal Government by investigating violations of criminal and civil law that adversely impact Federal tax administration, as well as administrative misconduct by IRS employees, all of which undermine the integrity of the Nation's voluntary tax system.

The Performance Model

The Office of Investigations accomplishes its mission through the hard work of its employees, whose efforts are guided by a performance model that focuses OI's resources on three primary areas of investigative responsibility:

- Employee integrity;
- Employee and infrastructure security; and,
- External attempts to corrupt tax administration.

The Office of Investigations has adopted performance measures that identify results derived from investigative activities that most accurately align with the strategic goals of the organization and that provide the greatest impact on the protection of the integrity of Federal tax administration.

The Council of the Inspectors General on Integrity and Efficiency awarded TIGTA special agents the Award for Excellence, in recognition of outstanding professionalism and unparalleled technological achievement by the Lost E-Mail Investigative Team for its efforts in conducting an unprecedented and complex investigation into the loss of electronic IRS records.

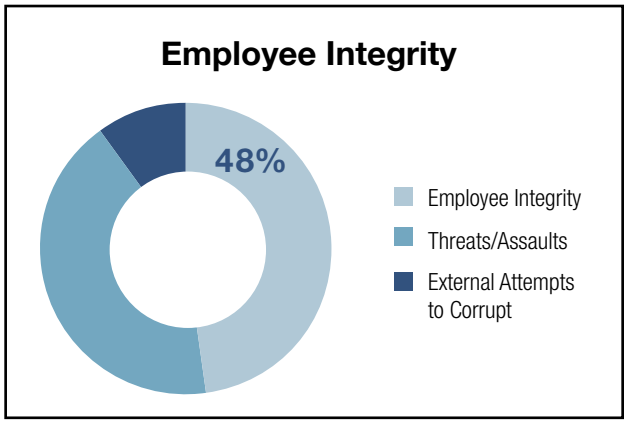
IRS employee misconduct undermines the IRS's ability to deliver taxpayer service, to enforce tax laws effectively, and to collect taxes owed to the Federal Government.

External threats against the IRS impede its ability to fairly, efficiently, and safely carry out its role as the Nation's revenue collector. Individuals who attempt to corrupt or otherwise interfere with the IRS through various schemes and frauds impact the IRS's ability to collect revenue.

TIGTA investigates these serious offenses and refers them to IRS management when they involve IRS employee misconduct. When appropriate, TIGTA also refers its investigations to the Department of Justice for prosecution.

Performance Area: Employee Integrity

In order for the country's tax system to succeed, taxpayers must have confidence in the fair and impartial administration of Federal tax laws and regulations. IRS employee misconduct, whether real or perceived, can erode the public's trust and impede the IRS's ability to effectively enforce tax laws.



Employee misconduct can take many forms, such as: the misuse of IRS resources or authority; theft; fraud; extortion; taxpayer abuse; unauthorized access to, and disclosure of, tax return information; and identity theft.

During this reporting period, employee integrity investigations accounted for 48 percent of OI's work.

Identity Theft and the Insider Threat

It is particularly troubling when IRS employees, who are entrusted with the sensitive personal and financial information of taxpayers, misuse their positions in furtherance of identity theft and other fraud schemes. This breach of trust negatively impacts our Nation's voluntary tax system and erodes confidence in the IRS. TIGTA proactively reviews the activities of IRS employees who access taxpayer accounts for any indication of unauthorized accesses that may be part of a larger fraud scheme.

The following cases represent OI's efforts to investigate identity theft committed by IRS employees during this six-month reporting period:

Former IRS Employee Indicted for Filing Fraudulent Tax Returns and Aggravated Identity Theft

On January 13, 2017, in the Western District of Missouri, former IRS employee Carla Mitchell was indicted for filing false tax returns and aggravated identity theft.[41]

According to the court documents, at all times relevant to the 15-count indictment, Mitchell was a contact representative at the IRS Service Center in Kansas City, Missouri. Mitchell was employed by the IRS from 2006 until June 2015, when she resigned. From at least February 2012 and continuing to about February 2014, Mitchell intentionally devised a scheme for the purpose of obtaining funds for herself and others by preparing false tax returns using false or stolen information to pay her own personal expenses and expenses for family members. In doing so, she knowingly and willfully aided and assisted in the preparation and presentation of Federal income tax returns, Form 1040, containing false information, and used the identification of another without lawful authority.[42]

Specifically, Mitchell prepared false tax returns for TYs 2011, 2012, and 2013 for approximately 13 of her friends and family members, as well as for herself. As part of her scheme, Mitchell included false entries to lower the individual tax liability or increase refunds for her friends, family members, and herself. These false entries included false wages and occupations, fraudulent Federal income tax withholdings, false Schedule C entries, fraudulent dependents, and false education expenses and credits.[43]

Mitchell prepared the false returns from her residence, her boyfriend's residence, and from the IRS Service Center in Kansas City. She charged approximately $150 each for the preparation of some of the returns, but did not sign the returns as a "paid preparer" and did not provide copies of the completed returns to friends and family members.[44]

Mitchell has been linked to 27 fraudulent returns with a total tax loss to the Government of approximately $118,012.19.[45]

---

41 W.D. Mo. Indict. filed Jan. 13, 2017.

42 Id.

43 Id.

44 Id.

45 Id.

Mitchell could face a maximum of three years' imprisonment as to each count of filing false tax returns, plus an additional mandatory two-year sentence for aggravated identity theft. Additional legal actions are anticipated.[46]

IRS Employee Sentenced for Conspiracy to Commit Identity Theft and Unauthorized Disclosure of IRS Records

On November 21, 2016, in the Western District of Tennessee, IRS employee Michael Anthony Jones was sentenced for conspiracy to commit identity theft and unauthorized disclosure of information.[47] Jones was initially charged with, and pled guilty to, the offense on July 19, 2016.[48]

According to the court documents, Jones, a resident of Memphis, Tennessee, was employed by the IRS as a contact representative at the IRS Service Center in Memphis. Jones had a personal relationship with his coconspirator, identified only as "TFB." Jones knowingly and willfully agreed and conspired with TFB and others to commit identity theft and unauthorized disclosure of information. The object of this conspiracy was for TFB to obtain IRS taxpayer information from Jones and use it for unjust financial enrichment.[49]

As part of the conspiracy, Jones used his access to the IRS databases, specifically the Remittance Transaction Research (RTR) system, to obtain taxpayer information without authorization.[50] According to the IRM, the RTR system provides access to remittance processing data and images, which generally include the front and back of a cancelled check or money order from a taxpayer, and a voucher if submitted with the payment.

Jones obtained RTR printouts of cancelled checks made payable to the U.S. Treasury Department and other personal information submitted by taxpayers to the IRS. Jones then disclosed such information to his coconspirator, providing TFB with the printouts and SSNs of at least three taxpayers for use in fraudulent activities. TFB used the illegally obtained information to breach taxpayers' bank accounts, obtain monies, and commit other financial fraud against the taxpayers and the IRS. Jones received a portion of the proceeds from TFB.[51]

---

46 Id.

47 W.D. Tenn. Judgment filed Nov. 21, 2016.

48 W.D. Tenn. Info. filed July 19, 2016; W.D. Tenn. Plea Agr. filed July 19, 2016.

49 W.D. Tenn. Info. filed July 19, 2016.

50 Id.

51 Id.

Jones was sentenced to two months in prison, followed by two years of supervised release. His supervised release will include two months of home detention, and Jones will participate in Moral Reconation Therapy.[52]

Employee Integrity

The following cases represent OI's efforts to ensure employee integrity during this six-month reporting period:

Former IRS Special Agent Indicted for Her Scheme to Impede the IRS

On October 20, 2016, in the Eastern District of California, former IRS Special Agent Alena Aleykina was charged in a superseding indictment with corrupt endeavor to impede the administration of the Internal Revenue laws, subscribing to false returns, theft of public funds, and destruction or falsification of records.[53]

According to the superseding indictment, Aleykina, a resident of Sacramento, California, was employed as an IRS Criminal Investigation special agent from approximately 2006 to 2014. Aleykina also was a Certified Public Accountant in the State of California and held a master's degree in Business Administration.[54]

From at least April 25, 2008 through April 15, 2013, Aleykina corruptly endeavored to execute a scheme to impede the due administration of the Internal Revenue laws by various means, which included submitting false Forms W-7, *Application for IRS Individual Taxpayer Identification Number*, on behalf of her family members in order to obtain IRS Individual Taxpayer Identification Numbers.[55] Furthermore, Aleykina established and used trusts and at least one partnership in her scheme, and prepared false and fraudulent Federal income tax returns for herself, her family members, and for the trusts and partnership. Additionally, she made false representations to representatives of the Department of the Treasury.[56]

Between 2010 and 2012, Aleykina prepared six false tax returns. Three of these returns were Aleykina's own individual income tax returns, and three were tax returns for trusts that she had established. All were signed under the penalties of perjury, and all contained false statements.[57]

---

52 W.D. Tenn. Judgment filed Nov. 21, 2016.

53 E.D. Cal. Superseding Indict. filed Oct. 20, 2016.

54 Id.

55 Id.

56 Id.

57 Id.

On Aleykina's individual tax returns, she falsely claimed head-of-household filing status. She also submitted claims for dependents to which she was not entitled, tuition and fees deductions, and losses of up to $25,000 for trusts that she had established. She knew all of these claims were false and was aware that she was not entitled to claim them. Aleykina stole public money and converted it to her own use by causing the IRS to issue IRS Tuition Assistance Reimbursement payments to her, knowing that she was not eligible for such money.[58]

The three estate and trust tax returns prepared by Aleykina also contained false information, including, but not limited to, the amounts of rents received, deductions of negative income distributions, and claims of negative net income identifying Aleykina as the beneficiary that were declared as losses on two of her corresponding individual tax returns.[59]

In April 2013, Aleykina knowingly destroyed, altered, concealed, and falsified at least one record that was stored on a Government-issued computer and Government servers.[60]

The charge of destruction of records in a Federal investigation carries a maximum penalty of 20 years' imprisonment.[61] Additional legal actions are anticipated.

Former IRS Employee Sentenced in Scheme Designed to Defraud the IRS and the Commonwealth of Pennsylvania

On January 12, 2017, in the Eastern District of Pennsylvania, former IRS employee Modestine Gillette, a/k/a "Cookie," was convicted of filing false claims, theft of Government property, aggravated identity theft, access device fraud, wire fraud, and filing a false Federal income tax return.[62] Gillette was indicted for the offenses in February 2015. Her daughter, Moniquetta Coats, was also charged with wire fraud in the February 2015 indictment.[63]

According to the court documents, Gillette was a seasonal contact representative working part-time at the IRS from October 2008 until March 2012. As a contact representative, Gillette was responsible for providing administrative and technical assistance to individuals and businesses that contacted the IRS with tax-related

---

58 Id.

59 Id.

60 Id.

61 Id.

62 E.D. Pa. Judgment filed Jan. 12, 2017.

63 E.D. Pa. Indict. filed Feb. 18, 2015.

questions. In her capacity as an employee, Gillette had access to IRS computerized files containing confidential tax return information for taxpayers, including names, SSNs, and income information. IRS employees are prohibited from accessing tax return information in the absence of an official business reason. Agency rules and regulations also prohibit employees from preparing tax returns for compensation. Gillette had received training and instruction in these legal obligations as a condition of her employment.[64]

In contravention of agency rules and regulations, Gillette prepared Federal income tax returns for friends, relatives, and acquaintances in exchange for payment. Between February 2010 and February 2012, Gillette knowingly prepared and filed, or caused to be filed, nine Federal income tax returns that contained false, fictitious, or fraudulent information, and diverted Government funds from those returns for her own benefit. Most of the individuals listed on the fraudulent tax returns had provided Gillette with their true income and expense information and had authorized Gillette to prepare and submit their returns. Nevertheless, the tax returns Gillette prepared and submitted to the IRS reported false information, including income not earned by the taxpayers, business expenses not incurred, false dependent claims, and inflated refund requests. The total amount claimed for income tax refunds was $34,466. One taxpayer did not authorize Gillette to prepare and submit a return on her behalf; however, Gillette used the taxpayer's identification to submit a fraudulent tax return and request an inflated refund. She then directed the inflated refund into a bank account in the name of her (Gillette's) spouse.[65]

Gillette knowingly stole and converted to her own use about $12,869 of the inflated refunds. Gillette did so by directing the taxpayers' refunds, or a portion thereof, into either her own bank account or, more often, into an account in the name of her spouse, generally without the taxpayers' knowledge.[66]

Further, since at least June 2010, Gillette was an owner or operator, and was employed by, A Unique Learning Experience, LLC (A Unique Experience), a child daycare business in Philadelphia, Pennsylvania. From about June 2010 through June 2013, Gillette devised a scheme to defraud the United States and the Commonwealth of Pennsylvania Department of Labor by obtaining money through false and fraudulent representations. Specifically, Gillette received benefits to which she was not entitled under the Federal Unemployment Program, the Emergency Unemployment Compensation Program, and the American Recovery and Reinvestment Act of 2009.

---

64 E.D. Pa. Indict. filed Feb. 18, 2015.

65 Id.

66 Id.

Gillette used the Internet and the telephone to submit applications and file claims falsely representing that she was not self-employed, was not working for any other employer, and had not worked for another employer in Pennsylvania since her separation from the Federal Government. Gillette failed to disclose that she had been receiving income from A Unique Experience. In 2011 alone, she received direct compensation from A Unique Experience in excess of $35,000. Gillette also failed to disclose that she was an owner and operator of A Unique Experience. As a result of these misrepresentations, Gillette received approximately 66 weeks of payments, totaling about $46,322, for unemployment benefits to which she was not entitled and which had been fraudulently obtained.[67]

Gillette's daughter, Coats, was also an owner, operator, and employee of A Unique Experience during the same time period. Coats similarly made fraudulent representations regarding her unemployment benefits by failing to disclose that she had been an owner and operator of A Unique Experience and by failing to disclose employment with, and income from, that business. As a result, Coats received about 16 weeks of unemployment payments to which she was not entitled, totaling approximately $10,578 in benefits.[68] Coats pled guilty on November 6, 2015,[69] to wire fraud related to the unemployment compensation fraud.

Moreover, in January 2012, Gillette willfully filed her own TY 2011 joint Federal income tax return, under penalty of perjury, knowing that it was not true and correct. Gillette failed to report as income: stolen funds of approximately $5,033, her income of about $35,138 from A Unique Experience, and her spouse's income from A Unique Experience in the amount of $3,929.[70]

Gillette was sentenced to a total term of imprisonment of 12 months and one day, to be followed by three years of supervised release. She was further ordered to pay restitution in the amount of $54,740.62. The terms of Gillette's supervised release include full cooperation with the IRS by filing of all delinquent or amended tax returns and by timely filing all future returns due during her period of supervision. Gillette is to properly report all correct taxable income and claim only allowable expenses and to refrain from preparing income tax returns.[71]

---

67 Id.

68 Id.

69 E.D. Pa. Crim. Docket filed Feb. 18, 2015

70 E.D. Pa. Indict. filed Feb 18, 2015.

71 E.D. Pa. Judgment filed Jan. 12, 2017.

Employee Integrity Projects

As part of its Employee Integrity focus, TIGTA conducts proactive investigative initiatives to detect misconduct in the administration of IRS programs. During this reporting period, TIGTA initiated 13 proactive projects to detect systemic weaknesses or potential IRS program vulnerabilities. TIGTA's most successful integrity project involves the detection of IRS employees who abuse their access to taxpayer information in order to commit identity theft and other crimes utilizing IRS information belonging to taxpayers.

Performance Area: Employee and Infrastructure Security

Collecting taxes is a critical function of the Federal Government. Threats and assaults directed at IRS employees, facilities, and infrastructure impede the effective and safe administration of the Federal tax system and the IRS's ability to collect tax revenue.

Through its investigations of threats directed toward the IRS, TIGTA also ensures a safe environment for taxpayers to conduct business with the IRS. All reports of threats, assaults, and forcible interference against IRS employees performing their official duties are referred to OI. During this six-month reporting period, OI responded to 771 threat-related incidents.

Contact with the IRS can be stressful and emotional for taxpayers. While the majority of taxpayer contacts are routine, some may become confrontational and even violent.

TIGTA's special agents are statutorily mandated to provide physical security, known as "armed escorts," to IRS employees who have face-to-face contact with a taxpayer who may pose a danger to the employee, and to ensure that IRS employees have a secure environment in which they can perform their critical tax administration functions. During this six-month reporting period, OI provided 36 armed escorts for IRS employees.

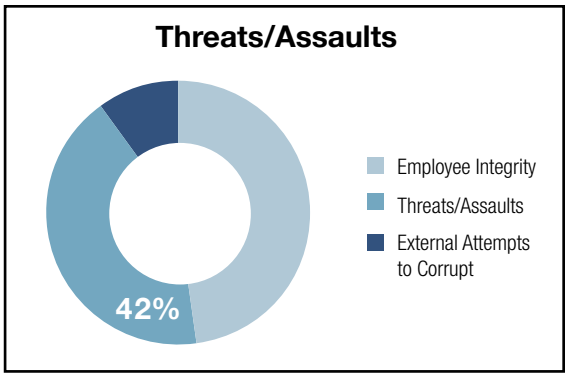
The Office of Investigations undertakes investigative initiatives to identify individuals who could commit violence against IRS employees or who could otherwise pose a threat to IRS employees, facilities, or infrastructure. It also provides intelligence to IRS officials to assist them in making proactive operational decisions about potential violence or other activities that could pose a threat to IRS systems, operations, and employees.

The investigative information sharing between OI and the IRS Office of Employee Protection (OEP) to identify potentially dangerous taxpayers is one example of TIGTA's commitment to protecting IRS employees. Taxpayers who meet OEP criteria are designated as potentially dangerous. Five years after this designation has

been made, TIGTA conducts a follow-up assessment of the taxpayer so that OEP can determine if the taxpayer still poses a danger to IRS employees.

During this six-month reporting period, threat and assault investigations accounted for 42 percent of OI's work.

The following case represents OI's efforts to ensure the safety of IRS employees during the reporting period:



Fort Lauderdale Man Sentenced for Forcibly Assaulting an IRS Employee With a Shotgun

On March 27, 2017, in the Southern District of Florida, Fort Lauderdale resident Bruce Hacker was sentenced for forcibly interfering with an employee of the U.S. Government.[72] Hacker was initially arrested[73] and charged with the offense in May 2016[74] and pled guilty in December 2016.[75]

According to the court documents, Hacker was charged with forcibly assaulting, intimidating, and interfering with an IRS revenue officer by using a deadly weapon, to wit, a shotgun, while the revenue officer was engaged in the performance of his official duties.[76] On May 19, 2016, the IRS revenue officer went to Hacker's residence in connection with an official IRS matter. The revenue officer identified himself and displayed his credentials to a female occupant who came to the door. After answering the door, the female told Hacker that an individual from the IRS was at the front door requesting to speak with him. Hacker said, "I'll take care of this" and retrieved his shotgun.[77] A short time later, Hacker opened the door, pointed the loaded shotgun at the revenue officer, shouted expletives at him, and told him to get off of his property, which the employee did.[78]

---

72 S.D. Fla. Judgment filed March 29, 2017.

73 S.D. Fla. Crim. Docket filed June 2, 2016.

74 S.D. Fla. Crim. Compl. filed May 20, 2016.

75 S.D. Fla. Plea Agr. filed Dec. 19, 2016.

76 Id.

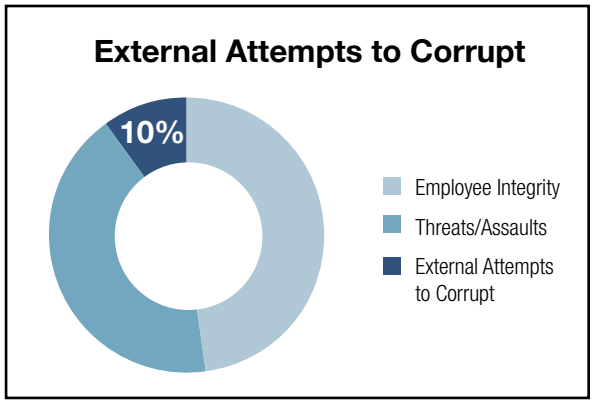
77 Id.

78 Id.

Hacker was no longer on the scene when law enforcement personnel proceeded to Hacker's residence, but a female was present. Special agents from TIGTA interviewed the female, who stated that the shotgun was loaded.[79] Hacker was sentenced to nine months in prison, followed by three years of supervised release.[80]

Performance Area: External Attempts to Corrupt Tax Administration

TIGTA also investigates external attempts to corrupt or impede tax administration. Taxpayers may interfere with the IRS's ability to collect revenue for the United States in many ways, for instance by: impersonating IRS employees or misusing IRS seals and symbols; filing false or frivolous documents against IRS employees; using fraudulent IRS documentation to perpetrate criminal activity; offering bribes to IRS employees to influence their tax cases; or committing fraud in contracts awarded by the IRS to contractors. These attempts to corrupt or otherwise interfere with tax administration not only inhibit the IRS's ability to collect revenue but also undermine the public's confidence in fair and effective tax administration.



Individuals may also impersonate IRS employees to obtain PII from unsuspecting taxpayers or to defraud them of their money. Such individuals may claim to be IRS employees on the telephone or may misuse IRS logos, seals, or symbols to create official-looking letters and e-mails. Impersonators often tell the taxpayers that they owe money to the IRS that must be paid through a preloaded debit card, wire transfer, or Apple® iTunes® gift card. Sometimes they trick taxpayers into providing their PII, which the impersonator uses to commit identity theft. TIGTA aggressively investigates these criminal activities to ensure that taxpayers maintain confidence in the integrity of Federal tax administration.

During this reporting period, investigations into attempts to corrupt or impede tax administration accounted for 10 percent of OI's work.

79 S.D. Fla. Factual Proffer for Change of Plea filed Dec. 19, 2016.

80 S.D. Fla. Judgment filed March 29, 2017.

Scams and Schemes

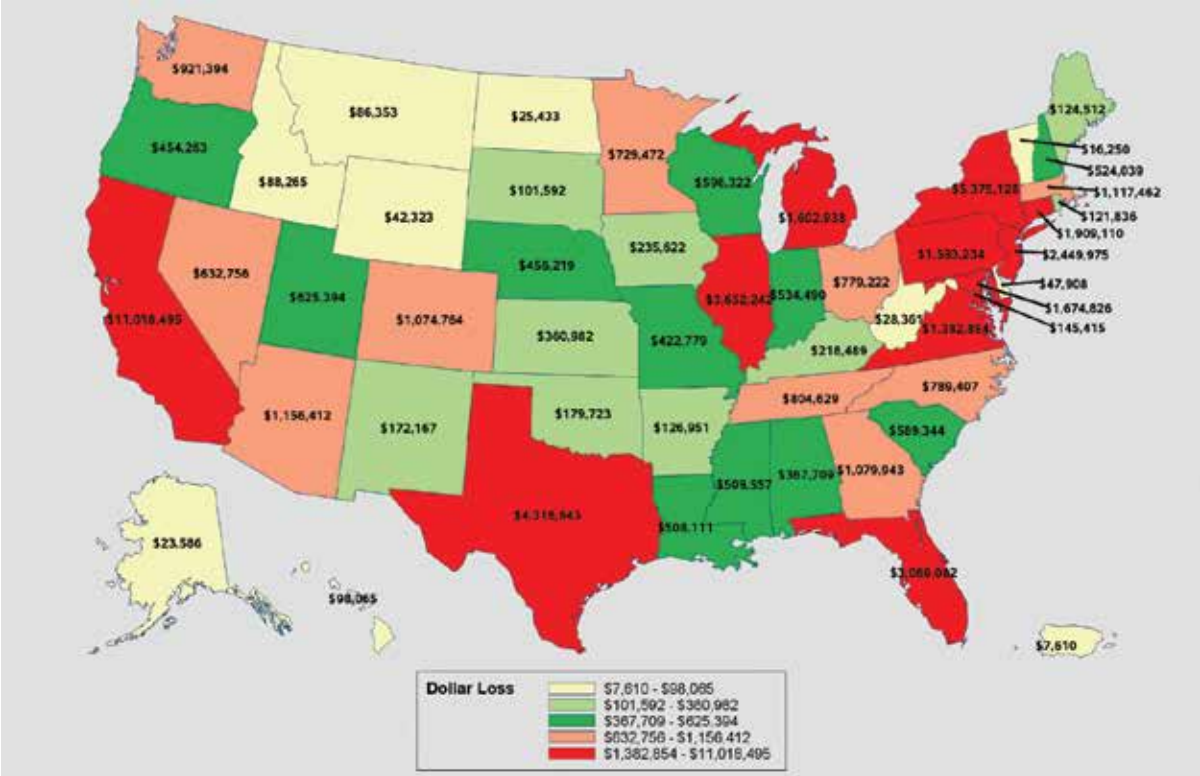
For more than 10 years, the IRS has provided the public with information on its website about what it deems to be the "Dirty Dozen" of tax scams. These scams range from falsely inflated deductions to fake charities and inflated refund claims. The list, which is compiled annually, features a variety of common scams that taxpayers may encounter. Many of these scams peak during the filing season, as people prepare their returns or utilize the services of paid preparers. The IRS telephone impersonation scam is, once again, included in the IRS's 2017 "Dirty Dozen" list.[81]

Between October 2013 and March 31, 2017, TIGTA logged more than 1.9 million contacts from taxpayers who reported that they had received telephone calls from individuals who claimed to be IRS employees. The impersonators told the victims that they owed additional tax and that if they did not immediately pay they would be arrested, lose their driver's licenses, or face other adverse consequences. As of March 31, 2017, more than 10,300 victims reported that they had paid the impersonators a total amount in excess of $55 million.

Because of their complexity, scams such as these are not typically resolved quickly. The impersonation scam has claimed victims in practically every State. The top five States with victims who have suffered financial losses are: California, Florida, Illinois, New York, and Texas.

81 https://www.irs.gov/uac/newsroom/dirty-dozen

Financial Losses by State



In addition to its investigative efforts, TIGTA has taken numerous other steps to combat this scam and protect taxpayers from being victimized. Specifically, OI created a three-pronged "Advise and Disrupt Strategy." The first part of this strategy involved analyzing and using the telephone numbers that victims reported to TIGTA. When a telephone number related to the impersonation scam was reported more than three times, OI special agents called it in order to confirm that an impersonator was on the other end of the line. If it was a confirmed part of the scam, OI identified the telephone carrier who owned the telephone number and requested that the carrier take the number down. Of the 1,180 telephone numbers OI identified using this method, 1,102 (93 percent) were successfully shut down, in some cases within a week of the numbers having been reported to us.

A second part of the strategy was to post scam-related telephone numbers on the Internet, which allowed potential victims to search to determine if the call they received was a part of the scam.

The final part of the strategy was to deploy a TIGTA auto-dialer to call back the impersonators with a message ordering them to cease and desist their criminal

activity, while also occupying the impersonators' time and telephone lines. The strategy resulted in over 143,000 auto-dialed calls back to the scammers.

Tax-related identity theft and IRS impersonation telephone scams cause a strain upon limited IRS and TIGTA resources and challenge the integrity of Federal tax administration.

TIGTA is also dedicated to educating the public about identity theft and IRS impersonation scams in its efforts to prevent fraud against the IRS and to protect U.S. taxpayers from falling prey to these scams. TIGTA has been working closely with the IRS, Federal Trade Commission (FTC), Federal Communications Commission (FCC), Consumer Protection Bureau, the Department of Veterans Affairs, U.S. Attorneys' offices, and a variety of State and local governments, as well as media outlets, to publish press releases, warnings, and other public awareness announcements to alert taxpayers to this scam.

TIGTA urges taxpayers to remain on "high alert" and continues to conduct outreach efforts to prevent them from falling victim to criminals who impersonate IRS and Treasury Department employees. The expanded outreach includes public service announcements (PSA), available on **YouTube** in English and Spanish, that warn taxpayers about the scam. The PSA videos have received over 71,000 views, and TIGTA has provided approximately 110 print and broadcast interviews, resulting in over 4,400 news stories in both large and small media markets, with an estimated audience size of roughly 113 million households, according to Nielsen rankings. Hundreds of messages warning about the scam are also appearing daily on other social media platforms, including Twitter. In addition, TIGTA provided testimony about the scams to two congressional committees.

The Office of Investigations is also working with its partners in the public and private sector to help get the word out, both through traditional law enforcement channels and through direct outreach to associations, nongovernmental organizations, and the media.

As part of its efforts with the FTC and the FCC, OI began working with the USTelecom Consortium and the RoboCall Task Force to identify how technology might be used to stop the spoofed calls that were being placed by the Indian call centers. In one successful pilot program, TIGTA and the Department of Homeland Security worked with Verizon to block almost two million calls that had been spoofed to appear as though the calls were being made from the IRS.

As the impersonation scam progressed, OI worked with the private sector companies that were caught in the middle of this massive fraud. The companies used by the impersonators to monetize the scam cooperated by using techniques to help warn consumers. For example, when a prepaid debit card is purchased, there is a fraud warning that now appears on the signature screen. Likewise, MoneyGram® has placed banners on its kiosks advising customers that if they have been told to pay their taxes by MoneyGram, it is a scam and they should not proceed with the transaction.

Since iTunes cards have been used 70 to 80 percent of the time by the impersonators as a means of cashing in on the fraud, Apple, Inc. (Apple) worked with TIGTA to create an audio message to help protect consumers. Apple also agreed to fund the nationwide distribution of this message at grocery and convenience stores, which resulted in more than 46 million consumers hearing this valuable message. Further, Wal-Mart Stores, Inc. has agreed to train its employees and post warning placards and fraud warning messages on cash envelopes.

> "Despite excellent progress we have made in our investigation of this matter, the callers are aggressive and relentless. Once they have your attention, they will say anything to con you out of your hard-earned cash. We continue to actively pursue those perpetrating this fraud, and we ask you to remain vigilant and report any calls you receive to our website."
>
> *– J. Russell George*
> *Treasury Inspector General for Tax Administration*
> *December 13, 2016*

Impersonation Scams

The following cases represent OI's efforts to investigate impersonation scams during this six-month reporting period:

Individual Pleads Guilty in Wisconsin to Conspiracy to Commit Wire Fraud

On January 19, 2017, in the Eastern District of Wisconsin, Harshkumar Rajnikant Patel pled guilty to conspiracy to commit wire fraud.[82] He and coconspirator Sunil Jashubhai Patel were initially charged in a 10-count indictment in July 2016.[83]

---

82 E.D. Wis. Plea Agr. filed Jan. 19, 2017.

83 E.D. Wis. Indict. filed July 26, 2016.

According to the court documents, beginning in approximately December 2015 and continuing through June 2016, the duo knowingly conspired with each other to commit wire fraud.[84]

In his plea agreement, Harshkumar Patel admitted that unknown members of the conspiracy located in India called victims and made misrepresentations causing the victims to send MoneyGram transfers. The callers pretended to be with law enforcement and informed the victims that they owed money to the IRS for unpaid taxes. The callers would tell the victims that they would be arrested and go to jail if the victims did not pay. The callers instructed the victims to send a certain amount of money to a specific location and to a specific fictitious name.[85]

Harshkumar Patel possessed fraudulent driver's licenses in the fictitious names of the MoneyGram recipients, but with a photo of himself. He used these fraudulent driver's licenses to pick up MoneyGram transfers, frequently several a day, from various locations. He knew where to pick up payments and which fraudulent driver's license to use because members of the conspiracy located in India would communicate that information to him. Harshkumar Patel was allowed to keep a certain percentage of the fraud proceeds and deposited the remaining cash into various bank accounts.[86] He used at least 12 different identities to receive over $650,000 in fraud proceeds from more than 600 transactions.[87]

Harshkumar Patel could face a maximum of 20 years' imprisonment.[88] His sentencing is scheduled for May 30, 2017.[89]

Nevada Trio Pleads Guilty in a Telemarketing Fraud Scheme Targeting the Elderly

On October 25, 2016, in the District of Nevada, Reginald A. Lowe, Willie J. Montgomery, and Tanika Armstrong all pled guilty in connection with a telemarketing fraud scheme.[90] Lowe and Montgomery pled guilty to conspiracy to commit wire or mail fraud in connection with a telemarketing scheme that was intended to target

84 Id; E.D. Wis. Plea Agr. filed Jan. 19, 2017.

85 E.D. Wis. Plea Agr. filed Jan. 19, 2017.

86 Id.

87 Id.

88 Id.

89 E.D. Wis. Crim. Docket as of Feb. 3, 2017.

90 D. Nev. Crim. Docket as of Nov. 18, 2016.

victims over the age of 55.[91] Armstrong pled guilty to conspiracy to commit money laundering for her role in the scheme.[92] All three were initially indicted and arrested in March 2016.[93]

According to the court documents, from November 2008 to September 2013, Lowe, Montgomery, and others devised a scheme to defraud and obtain money by means of false and fraudulent pretenses. In furtherance of the conspiracy, Montgomery, Lowe, and others obtained "lead sheets," which identified persons who had previously entered sweepstakes, lotteries, or other prize-drawing contests and who were thus thought to be susceptible to misrepresentations regarding potentially winning a prize, sweepstakes, or lottery. The defendants knew these leads typically consisted of contact information for elderly or retirement-age people or others who were particularly vulnerable or susceptible to schemes.[94]

Using the lead sheet information, the conspirators, in the role of "talkers," would contact potential victims by telephone and falsely represent to them that they had won prizes consisting of large amounts of cash or other high-value merchandise. In doing so, the talker would hold himself out as being an official or employee of a lottery/sweepstakes committee or a Government regulatory authority. The talker would frequently represent himself to be an official or employee of the IRS. The talker would tell the victim that in order to receive the prize, he or she must first send money as payment for taxes on prize winnings or other fees. Lowe, Montgomery, and their coconspirators knew at all times that the victims had not actually won any prizes or things of value and would receive nothing for their payments.[95]

The talker would direct the victim to send payment in the form of checks, money orders, U.S. currency, or other negotiable instruments via Western Union or MoneyGram wire transfer, U.S. Postal Service®, United Parcel Service (UPS)®, or FedEx®. Lowe and Montgomery used individuals referred to as "runners" to retrieve the payments and deliver the money to them and their coconspirators. The runners were given a small percentage of the criminal proceeds.[96]

The defendants caused victims to send approximately $96,983 via MoneyGram and at least $366,238 via Western Union wire transfers. The defendants also fraudulently

---

91 D. Nev. Plea Agr. filed Oct. 25, 2016; D. Nev. Plea Agr. filed Oct. 25, 2016.

92 D. Nev. Plea Agr. filed Oct. 25, 2016.

93 D. Nev. Indict. filed Mar. 16, 2016; D. Nev. Arrest Warrant filed March 23, 2016; D. Nev. Arrest Warrant filed March 24, 2016; D. Nev. Arrest Warrant filed March 25, 2016.

94 D. Nev. Plea Agr. filed Oct. 25, 2016.

95 Id.

96 Id.

induced the victims to send a total of at least $389,924 through the U.S. mail, UPS, and FedEx.[97]

During the course of the scheme, Montgomery's wife, Tanika Armstrong, was provided with money orders to deposit and convert to cash. Armstrong opened a bank account in the name of a limited liability company in order to launder the monetary instruments and conceal the criminally derived origins. Armstrong did so with full knowledge that the proceeds were fraudulently obtained.[98]

In total, the conspirators fraudulently obtained approximately $1,175,670 from the scheme, which claimed at least 66 victims from 22 different States.[99]

Lowe and Montgomery both agreed to make restitution to victims of the scheme in the full amount of $1,175,670.21.[100] As part of her plea agreement, Armstrong agreed to make restitution in the amount of $18,475 to victims.[101]

The maximum penalty for each of the offenses is 20 years' imprisonment. Lowe and Montgomery were scheduled to be sentenced on January 25, 2017;[102] however, on or about January 14, 2017, Lowe passed away.[103] Montgomery and Armstrong are now scheduled for sentencing in April 2017.[104]

Two Individuals Convicted in New York for Their Roles in Jamaican Lottery Schemes

On October 11, 2016, in the Southern District of New York, Daile Ferguson, a/k/a Normandale Ferguson,[105] was convicted and sentenced for conspiracy to commit wire fraud[106] in connection with a Jamaican lottery scheme.[107] Ferguson had been arrested in December 2015 for the offense and pled guilty in May 2016.[108]

---

97 Id.

98 D. Nev. Plea Agr. filed Oct. 25, 2016.

99 D. Nev. Plea Agr. filed Oct. 25, 2016.

100 D. Nev. Plea Agr. filed Oct. 25, 2016; D. Nev. Plea Agr. filed Oct. 25, 2016.

101 D. Nev. Plea Agr. filed Oct. 25, 2016.

102 D. Nev. Crim. Docket as of Nov. 18, 2016.

103 D. Nev. Stipulation to Continue Sentencing Date filed Jan. 20, 2017.

104 D. Nev. Crim. Docket as of Jan. 25, 2017.

105 S.D. N.Y. Crim. Docket as of Oct. 20, 2016.

106 S.D. N.Y. Judgment filed Oct. 12, 2016.

107 S.D. N.Y. Indict. filed Feb. 17, 2016.

108 S.D. N.Y. Crim. Docket as of Oct. 20, 2016.

According to the court documents, Ferguson, who entered the United States using a Jamaican passport, was involved in a scheme to obtain money from elderly victims by informing them that they had won substantial cash prizes in an international sweepstakes lottery, but that before they could claim their prizes they had to pay fees and taxes. The victims were contacted by telephone, fax, and e-mail and were requested to pay fees and taxes on the winnings; however, there was no sweepstakes lottery and the victims never received any cash prizes. The victims sent hundreds of thousands of dollars in cash and checks to conspirators in the United States and in Jamaica. Ferguson received more than $430,000 from approximately 87 different individuals throughout the United States. Approximately 43 victims were over 70 years old and approximately 59 were over 60 years old.[109]

One of the victims, a resident of Connecticut, received a letter purporting to be from a "tax return officer" with the IRS. That letter advised that the victim had won $750,000, which was processed through the IRS office, and stated that the IRS "has also verified and has recorded the payment." The letter also stated that insurance fees had to be paid before the victim could receive the money. Additionally, the victim received several telephone calls from various individuals, including an individual who identified herself as an employee of the IRS and demanded that the victim make payments in order to receive the supposed winnings. As a result of the telephone calls and e-mails that the victim received from the conspirators, the victim sent approximately $20,000 through various means to numerous individuals, including Daile Ferguson.[110]

When interviewed, Ferguson admitted that, in or around 2011, he began collecting money from individuals located in the United States on behalf of his acquaintances in Jamaica and kept for himself a portion of the money he collected. He also admitted that he heard that at least one of the individuals on whose behalf he collected money was involved in a lottery scheme. He admitted that "something felt wrong" and "not right" about collecting the money.[111]

Ferguson was sentenced to 33 months in prison, followed by three years of supervised release. Ferguson was further ordered to pay restitution to the victims in the amount of $439,386.79. He was ordered to surrender to the Bureau of Prisons on January 17, 2017.[112]

---

109 S.D. N.Y. Crim. Compl. filed Dec. 16, 2015.

110 Id.

111 Id.

112 S.D. N.Y. Judgment filed Oct. 12, 2016.

In another case, Adrian Foster, who also entered the United States with a Jamaican passport,[113] was convicted and sentenced in the Southern District of New York on January 12, 2017, for conspiracy to commit wire fraud.[114] Foster was indicted in June 2016[115] and pled guilty to the offense in October 2016.[116]

According to the court documents, from at least 2009 until at least 2014, Foster and others participated in a telemarketing scheme to defraud victims, many of whom were elderly. Members of the conspiracy located in Jamaica purchased lists containing the names, contact information, and ages of individuals living in the United States. They then telephoned these individuals and informed them that they had won the lottery but that they must pay various taxes and fees prior to receiving their winnings.[117]

Based on these false representations, some of the victims sent cash or checks to Foster and others. One such victim from Ohio received a telephone call from an individual in Jamaica who represented that the victim had won the lottery. According to the criminal complaint, the victim was sent letters purporting to be on IRS letterhead and was asked to send funds for taxes, insurance, and money releases. The victim subsequently received a number of additional phone calls purportedly related to the sweepstakes. As a result of the phone calls and written correspondence, the victim sent tens of thousands of dollars, including a certified check made out to Adrian Foster in the amount of $60,000, but did not receive any winnings. Foster had been arrested, along with several coconspirators, in Jamaica in late 2009 for suspected involvement in a lottery scam. He was found with documents linking him and his coconspirators to the scam, including the $60,000 check from this victim. The Jamaican charges were ultimately dismissed because the victim was unable to travel to Jamaica to testify.[118]

Another victim, born in 1925 and residing in California, was contacted and informed that she had won $4.5 million in the lottery. This victim received written correspondence from an individual claiming to be employed by the IRS. The victim said that the IRS contact was scheduled to bring a $795,000 check and a car worth $72,000 to her on a specified date. No one called or visited the victim on that date. The victim's financial records revealed that large sums of money, at least $570,000,

---

113 S.D. N.Y. Crim. Compl. filed Mar. 11, 2016.

114 S.D. N.Y. Judgment filed Jan. 13, 2017.

115 S.D. N.Y. Indict. filed June 13, 2016.

116 S.D. N.Y. Crim. Docket as of Oct. 20, 2016.

117 S.D. N.Y. Indict. filed June 13, 2016.

118 S.D. N.Y. Crim. Compl. filed Mar. 11, 2016.

had been wired to two of Foster's coconspirators. Additionally, Western Union transactions were made from one of these coconspirators to Foster.[119]

In total, Foster and his coconspirators defrauded their victims of more than $1 million during the course of the conspiracy.[120]

Foster was sentenced to 15 months' incarceration, followed by three years of supervised release,[121] and was ordered to forfeit $23,940.[122] On January 23, 2017, Foster was further ordered to pay restitution to the victims in the amount of $72,540.95.[123]

Corrupt Interference

The following cases represent OI's efforts to address and deter external attempts to corrupt tax administration during this six-month reporting period:

Florida Man Impersonates an IRS Employee in Attempt to Evade Income Tax

On November 28, 2016, in the Middle District of Florida, Steven Headden Young was sentenced for attempting to evade or defeat Federal tax laws.[124] Young was initially charged with, and pled guilty to, the offense in April 2016.[125] According to the court documents, Young, who was a resident of Tampa, Florida, during the relevant time periods, knowingly and willfully attempted to evade and defeat the income tax due and owing by him to the United States. Young committed a number of affirmative acts of tax evasion, including: filing false Federal tax returns, concealing income, making false deductions for non-existent expenses, making false statements about his filing status, and making false claims to refunds.[126]

Additionally, Young interfered with an IRS audit of his taxes by impersonating an IRS employee, in an attempt to intercept and take from the IRS summonsed third-party records for the IRS audit and tax assessment of Young's personal Federal income

---

119 Id.

120 S.D. N.Y. Indict. filed June 13, 2016.

121 S.D. N.Y. Judgment filed Jan. 13, 2017.

122 S.D. N.Y. Consent Order of Forfeiture filed Jan. 13, 2017.

123 S.D. N.Y. Order of Restitution filed Jan. 23, 2017.

124 M.D. Fla. Judg. filed Nov. 29, 2016.

125 Id.

126 Id.

taxes.[127] Purporting to be an IRS employee, Young sent a fraudulent letter to Bank of America in an effort to intercept records related to his bank accounts that had been summonsed by an IRS revenue agent. In the letter, Young falsely stated that the address for the IRS revenue agent had been changed to an address where Young had opened a post office box at a UPS store in the name of the IRS revenue agent. Young had presented a false Allstate Insurance Company card and voter's registration card in the name of another IRS employee in order to open the post office box.[128]

Young was sentenced to 21 months in prison, followed by three years of supervised release. He was further ordered to pay restitution to the IRS in the amount of $509,444.18, to cooperate with the IRS by providing lawful tax returns for TYs 2007 through 2011, and to pay all outstanding tax, interest, and penalties.[129]

Three Individuals Plead Guilty to the Theft of a $4.3 Million Treasury Check

On January 30, 2017, in the Northern District of Georgia, Renina Letricia Wortham, a/k/a Renina Simmons-Wortham, and Prentice Johnson each pled guilty to the theft of public money, to wit, a U.S. Treasury check in the amount of $4,368,869.30.[130] A third individual, Enobahkare Peterson, also pled guilty on January 26, 2017.[131] All three had been initially charged in November 2016.[132]

According to the court documents, the check was confirmed to be a U.S. Treasury check that had been issued to HR Outsourcing Associates, Inc. (HROA) on August 23, 2016. HROA is a payroll processor handling the IRS filings of corporate clients. It has over 400 corporate clients, most of which have many individual employees. The check was issued in association with payroll tax overpayments of HROA clients.[133]

HROA stated that only two people in the company would have had access to such a Treasury check. Johnson, a former HROA Payroll Manager in Lawrenceville, Georgia, was identified as one of those people. He had been employed with HROA for approximately two and a half years before he was let go on September 16, 2016, after the company consolidated payroll processing. He knew he was being laid off from the company, but continued to work and had access to HROA records, tax notices,

---

127 M.D. Fla. Plea Agr. filed Apr. 20, 2016.

128 M.D. Fla. Plea Agr. filed Apr. 20, 2016.

129 M.D. Fla. Judgment filed Nov. 29, 2016.

130 N.D. Ga. Plea Agr. filed Jan. 30, 2017; N.D. Ga. Indict. filed Jan. 3, 2017; N.D. Ga. Crim. Info. filed Jan. 4, 2017.

131 N.D. Ga. Plea Agr. filed Jan. 26, 2017.

132 N.D. Ga. Crim. Compl. filed Nov. 10, 2016.

133 Id.

and Treasury checks in the mail during the time the $4.3 million Treasury check was mailed to HROA.[134]

Johnson and Wortham are believed to be family members or close associates. Peterson said he met a lady identified as Wortham at a car dealership. She brought the Treasury check and asked him if he had some way to negotiate it. She had an inside person who filed returns for corporations. Peterson then asked other individuals to help find a way to negotiate the stolen U.S. Treasury check. Peterson said that there were actually $58 million in checks, and the $4.3 million check was the smallest.[135]

The individuals met with Wortham, who mentioned that there were approximately 22 additional Treasury checks. The checks were stolen from an accounting firm that files taxes for other companies, and the company appearing on the front of the checks had no idea that they were even missing. Wortham stated that this opportunity had presented itself because of a family member that she tried to help along the way. One of the individuals stated that Wortham passed him the Treasury check.[136]

Each of the defendants could face a maximum of 10 years in prison. Peterson is scheduled to be sentenced on April 5, 2017.[137] Johnson and Wortham are both scheduled for sentencing on May 1, 2017.[138]

Postal Employee and Spouse Indicted for Passing Forged Endorsements on U.S. Treasury Checks and Threatening a Federal Law Enforcement Officer, Respectively

On February 7, 2017, in the Central District of California, Jill Louise Lewis and Darren Adrian Lewis were indicted for conspiracy and embezzlement of money orders. Jill Lewis was also indicted for passing forged endorsements on U.S. Treasury checks, and Darren Lewis for threatening a Federal law enforcement officer.[139] The husband and wife[140] were both arrested on January 25, 2017, for the offenses.[141]

---

134 Id.

135 Id.

136 Id.

137 N.D. Ga. Crim. Docket as of Feb. 1, 2017.

138 N.D. Ga. Crim. Docket as of Feb. 1, 2017; N.D. Ga. Crim. Docket as of Feb. 1, 2017.

139 C.D. Cal. Indict. filed Feb. 7, 2017.

140 C.D. Cal. Crim. Compl. filed Jan. 23, 2017.

141 C.D. Cal. Crim. Docket filed Feb. 7, 2017.

According to the court documents, Jill Lewis, Darren Lewis, and others conspired to defraud by passing U.S. Treasury checks with forged endorsements and by embezzling, stealing, and knowingly converting to their own use, without authority, money orders provided by the U.S. Postal Service.[142]

As part of the conspiracy, Jill Lewis would steal U.S. Treasury checks payable to other persons from the mail at the U.S. Post Office in Littlerock, California, where she worked. She would then falsely endorse the stolen Treasury checks at her service window and exchange them for cash or postal money orders made payable to herself, her husband, and other coconspirators. Jill Lewis, Darren Lewis, and others would take these money orders and either cash them at post offices in Littlerock, Palmdale, or Lancaster, California, or deposit the money orders into Jill Lewis's bank accounts.[143]

For instance, in July 2016, Jill Lewis falsely endorsed a U.S. Treasury check in the amount of $4,961 in the name of another person and exchanged it for five postal money orders in various amounts, all made payable to Darren Lewis. Darren Lewis then cashed the five money orders at two separate post office locations. Jill Lewis falsely endorsed Treasury checks totaling more than $14,300.[144] During an interview with law enforcement agents, she admitted that she stole approximately eight Treasury checks and a "handful" of gift cards from the mail at the post office where she worked. She further explained how her husband helped her deposit the stolen funds.[145]

During his interview with law enforcement agents, Darren Lewis admitted his complicity in Jill Lewis's fraudulent use of Treasury checks, as well as his role in "washing" the checks that were stolen from the mail.[146] Darren Lewis also knowingly threatened to assault a Federal law enforcement officer with the intent to impede, intimidate, and interfere with the agent while engaged in the performance of official duties and with the intent to retaliate against the agent on account of the performance of official duties.[147] Specifically, Darren Lewis said he knew people who could harm the agent and the agent's family. He divulged that he had purchased an iPad mini™ the night before the interview in order to research the agent's personal information using a new digital device so that the Internet Protocol (IP) address would not be traced back to him. He admitted that he had looked up the agent's

---

142 C.D. Cal. Indict. filed Feb. 7, 2017.

143 Id.

144 Id.

145 C.D. Cal. Crim. Compl. filed Jan. 23, 2017.

146 Id.

147 C.D. Cal. Indict. filed Feb. 7, 2017.

home address so that he could ask others to cause harm to the agent and the agent's family.[148]

Additional legal actions are anticipated for Jill and Darren Lewis.

Louisiana Man Indicted for Bank Fraud and Obstructing the Due Administration of the Internal Revenue Laws

On November 16, 2016, in the Middle District of Louisiana, Adrian C. Hammond, Jr. was indicted for obstructing the due administration of the Internal Revenue laws, bank fraud, false statements to a bank, and money laundering.[149]

According to the indictment, Hammond, a resident of Baton Rouge, Louisiana, owned and/or operated a number of businesses, including: 51/50 Productions, LLC; Northgate Investments, LLC; Black Gold Rush, LLC; and Best Boilers Seafood, LLC. From about August 2011 through June 2015, Hammond knowingly executed a scheme to defraud Fidelity Bank, later known as Red River Bank. Hammond did so by means of materially false and fraudulent pretenses and representations, including providing the bank with a false financial statement and tax returns purportedly filed with the IRS, in order to obtain money, assets, and other property from the bank for his own unlawful enrichment.[150]

In reality, Hammond had an unpaid balance due to the IRS for taxes owed, dating back as far as TYs 2003 and 2006. The IRS had entered assessments against Hammond for his unpaid tax debt on various dates in 2007 and 2010. In 2011, Hammond owed an additional sum to the IRS, bringing the total amount of his unpaid tax debt to more than $105,000. When Hammond failed to pay any of his outstanding tax liability, the IRS filed a Notice of Tax Lien against him for $114,758.62 in the 19th Judicial District Court for East Baton Rouge Parish in September 2011.[151]

From approximately October 2011 through August 2014, Hammond corruptly endeavored to impede and obstruct the due administration of the Internal Revenue laws by making false representations to the IRS and others regarding the status of his unpaid tax liability. This was done to unjustly enrich himself and to gain an unjust advantage over honest businesspeople who paid their taxes.[152]

---

148 C.D. Cal. Crim. Compl. filed Jan. 23, 2017.

149 M.D. La. Indict. filed Nov. 16, 2016.

150 Id.

151 Id.

152 Id.

Between October and December of 2011, Hammond made numerous false representations to the IRS about his ability and intent to pay his unpaid tax liability. Hammond represented that he was close to securing a loan for his business and would also pay off the IRS lien in full. Based on his representations, the IRS agreed to withdraw the tax lien. Hammond, however, did not pay his outstanding tax liability over the next two years. Furthermore, during 2012, Hammond contacted the IRS revenue officer assigned to his case and claimed to have on the phone with him an individual whom he identified as a "Vice President" at Fidelity Bank. The individual represented that Fidelity's loan to Hammond was moving forward. The IRS once again agreed to postpone Hammond's deadline for repaying his debt. In fact, the individual posing as a bank official during the call did not work for Fidelity Bank. By March 2013, Hammond's tax liability remained outstanding, and the IRS filed another Notice of Tax Lien against him in the District Court.[153]

In 2014, the IRS served a Notice of Levy on a tenant living on rental property that Hammond owned, in effect instructing the tenant to mail any rental payments to the IRS instead of Hammond. Hammond then falsely represented to the tenant that the IRS had released the levy and that he was paying the IRS.[154]

Subsequently, around August 2014, Hammond created a fraudulent document, which appeared to be a second withdrawal of the Federal tax lien that had been filed against Hammond in 2013. Hammond caused the fraudulent document to be filed in the 19th Judicial District Court, thereby concealing the existence of the lien from public records checks. Hammond, in fact, knew the IRS had not prepared, approved, or executed this withdrawal and that it did not wish to remove the lien, which it had properly filed and recorded.[155]

Additional legal proceedings are anticipated in the case.

Georgia Man Arrested for Wire Fraud

On December 1, 2016, in the Northern District of Georgia, Alphonso I. Waters, Jr. was arrested[156] for wire fraud related to his role in a scheme to defraud a financial institution.[157] Waters was indicted for wire fraud on November 21, 2016.[158]

---

153 Id.

154 Id.

155 Id.

156 N.D. Ga. Executed Arrest Warrant filed Dec. 8, 2016.

157 N.D. Ga. Indict. filed Nov. 21, 2016.

158 Id.

According to the indictment, Waters and his wife, identified as "Dr. S.M.W.," owned and operated Family Practice of Atlanta Medical Group, LLC, a medical practice in Decatur, Georgia. Waters was the chief operating officer, chief financial officer, and manager of the medical practice.[159]

In 2011, Waters secured financing through JPMorgan Chase Bank to construct a commercial medical building in Decatur and, in July 2013, renewed two promissory notes with JPMorgan Chase. In about October 2013, Waters sought additional funding for the construction project in the amount of $6 million from Colony Capital Acquisitions, LLC (Colony), a private mortgage lending business. When seeking the loan from Colony, Waters falsely stated that neither he nor his wife had any unpaid taxes or liens, when, in fact, Waters and his spouse owed Federal taxes for TYs 2007 through 2012 and were the named taxpayers in two Federal tax liens filed in the Superior Court of Fulton County, Georgia.[160]

After Colony discovered the Federal tax liens, Waters caused his accountant to request the assistance of the IRS Taxpayer Advocate Service to establish a payment plan to resolve his and his wife's outstanding tax liability. He further caused a letter to be submitted to the IRS by his attorney in an attempt to expedite the approval of a payment plan for the unpaid Federal tax liens and contacted his local congressman to request assistance in expediting a payment plan with the IRS.[161]

When the IRS faxed to his accountant notice of an estimated resolution date of March 31, 2014, Waters knowingly caused a false and fraudulent letter to be faxed to Colony stating that Waters' requested payment plan had been approved. The fraudulent letter was purportedly from the IRS Office of the Chief Counsel in Washington, D.C., bearing the signature of "Rebecca Langford, District Director." In fact, the IRS did not have a current or former employee by this name, and no IRS employee was assigned the title of "District Director."[162]

In an attempt to conceal the scheme to defraud, Waters subsequently sent an e-mail to the congressman's office thanking the office for its assistance in expediting approval for a payment plan with the IRS, knowing that the IRS letter was fake and that the congressman's office had not provided assistance in expediting the approval.[163]

---

159 Id.

160 Id.

161 Id.

162 Id.

163 Id.

Additionally, in a further attempt to conceal the scheme to defraud, Waters caused to be sent to Colony a letter signed by Waters stating that, to the best of his knowledge, the IRS letter was from Rebecca Langford, IRS District Director, well knowing that the IRS letter was fake and fraudulent, all in an attempt to secure the $6 million Colony loan.[164]

Wire fraud carries a maximum statutory sentence of 20 years' imprisonment. Additional legal proceedings are anticipated.

Tax Preparer Outreach

In addition to promoting employee integrity, TIGTA is also committed to educating tax preparers on integrity. Tax preparers play an important role in ensuring the integrity of tax administration because of their frequent contact with the IRS; they also are often the first line of defense for maintaining a professional image and reputation in the preparer community.

During this semiannual reporting period, TIGTA special agents provided 17 integrity presentations to tax preparers at various locations nationwide. The presentations generally informed tax preparers of TIGTA's role in protecting the integrity of tax administration, differentiating between TIGTA's jurisdiction and the IRS's, identifying various forms of preparer misconduct, and describing common IRS impersonation scams.

These outreach efforts are important due to the influence that tax preparers have on tax compliance or noncompliance. Tax preparers can either assist in the enforcement of tax administration by ensuring taxpayers' compliance with Internal Revenue laws or they can impede it.

The following cases represent OI's efforts to protect tax administration from unscrupulous tax preparers during this six-month reporting period:

North Carolina Tax Preparer Pleads Guilty to Corruptly Endeavoring to Impede the IRS and Tax Evasion

On October 4, 2016, in the Middle District of North Carolina, tax preparer Henti Baird pled guilty to corruptly endeavoring to impede the IRS and tax evasion.[165]

---

164 Id.

165 M.D. N.C. Crim. Docket filed Sept. 27, 2016; M.D. N.C. Plea Agr. filed Sept. 29, 2016.

According to the court documents, Baird, a resident of Greensboro, North Carolina, owned and operated HL Baird Tax Consultants. For nearly forty years, Baird had worked extensively with the IRS, serving for 12 years as a revenue officer for the Collection Division for the IRS in the 1970s and 1980s.[166] The business advertised that it provided various tax services, including tax preparation and representing clients in matters before the IRS,[167] and that it specialized in IRS problems.[168] From July 1998 until April 2009, the IRS authorized Baird as an enrolled agent, which allowed him to represent taxpayers before the IRS and required him to complete continuing education courses.[169]

From about January 2008 through about October 2013, Baird corruptly endeavored to obstruct and impede the due administration of the Internal Revenue laws by various acts. These included filing Forms 2848, *Power of Attorney and Declaration of Representative*, on behalf of taxpayers after the IRS had terminated his enrolled agent status, using another person's name and SSN to apply for and use a Preparer Tax Identification Number (PTIN) to file returns for taxpayers, and hiding his income and assets to evade the payment of individual taxes owed.[170]

Specifically, the IRS Form 2848 authorizes an individual to represent a taxpayer before the IRS. The representative must be eligible to practice before the IRS. Baird filed at least 120 Forms 2848, on which he signed, under penalties of perjury, that he was an enrolled agent. However, in 2009 the IRS revoked Baird's status as an enrolled agent.[171] Additionally, in 2011 and 2012, Baird filed a renewal application for a PTIN using the SSN and name of his stepson without his knowledge. A PTIN is the number the IRS assigns to those who prepare or assist in the preparation of Federal tax returns for compensation.[172] Baird then prepared and filed over 900 tax returns for clients using the PTIN.[173]

Despite Baird's knowledge of his tax obligations, he failed to pay the taxes that he self-assessed and, as of September 2016, owed income taxes of approximately $477,028.80 for TYs 1998 through 2013. The IRS attempted several times to levy Baird's bank

---

166 M.D. N.C. Factual Basis filed Sept. 29, 2016.

167 M.D. N.C. Info. filed Sept. 27, 2016.

168 M.D. N.C. Factual Basis filed Sept. 29, 2016.

169 Id.

170 M.D. N.C. Info. filed Sept. 27, 2016.

171 M.D. N.C. Factual Basis filed Sept. 29, 2016.

172 M.D. N.C. Info. filed Sept. 27, 2016.

173 M.D. N.C. Factual Basis filed Sept. 29, 2016.

accounts, but those attempts resulted in minimal recovery.[174] Baird responded to the liens and levies by using his knowledge of the IRS collection process to delay and impede the IRS's efforts. Baird willfully attempted to evade and defeat the payment of an income tax due and owing by him by: engaging in numerous ploys, including telling the investigating revenue officer that he did not have an account at a specific bank, when in reality he controlled multiple accounts at this bank; sending two estimated tax payments to the IRS for $18,000 each, both of which were returned for insufficient funds; and making substantial cash deposits into various bank accounts in the names of his adult children.[175]

Baird could face a maximum of five years' imprisonment. His sentencing is scheduled for April 28, 2017.[176]

New Jersey Tax Preparer Indicted for Aiding and Assisting in the Filing of False Tax Returns and Bank Fraud

On February 1, 2017, in the U.S. District Court, District of New Jersey, tax preparer Brian A. Day was indicted for aiding and assisting in the filing of false tax returns and bank fraud in connection with a scheme to defraud and to misappropriate his clients' monies.[177]

According to the court documents, Day, a resident of Port Murray, New Jersey, was self-employed as a tax return preparer. Day was the sole owner and operator of various tax preparation businesses located in Essex County, New Jersey, including PTS, Tax Consultants, and Tax Consultants, LLC. Day met with taxpayers at his offices and collected information relating to the preparation of their individual income tax returns.[178]

The indictment charges that from about December 2011 through April 2015, Day knowingly and intentionally executed a scheme to defraud and obtain money by means of false and fraudulent representations. The purpose of the scheme was for Day to misappropriate money from his taxpayer clients by falsely advising them that they owed tax payments to the IRS and directing them to give him checks made payable to the IRS to resolve the purported IRS liabilities. In fact, Day did not actually give the checks from his taxpayer clients to the IRS. Instead, he altered the checks

---

174 M.D. N.C. Info. filed Sept. 27, 2016.

175 M.D. N.C. Factual Basis filed Sept. 29, 2016; M.D. N.C. Info. filed Sept. 27, 2016.

176 M.D. N.C. Crim. Docket as of Feb. 27, 2017.

177 D. N.J. Indict. filed Feb. 1, 2017.

178 Id.

from the "IRS" to names matching or resembling the names of his tax preparation businesses and deposited the checks into his own business bank account. Using this means, Day accepted payments from three clients totaling at least $61,000 to settle tax liabilities.[179]

When Day's clients discovered that he had not paid the IRS with the checks they had given him, they attempted to contact him. Day either did not respond to their calls or, in order to conceal and further his scheme, he presented his clients with fraudulent documents purportedly issued by the IRS. Day presented one taxpayer with a fake letter which purported to be from the IRS. The letter falsely confirmed that the IRS had received a payment of $11,000 from the taxpayer and falsely stated that $880 was still due and that the taxpayer owed an additional penalty payment of $6,286. Day presented another taxpayer with a fake letter, which purported to be from the IRS, stating that the IRS had received a payment of $5,000 from the taxpayer and that the taxpayer's case was now closed. The IRS never issued the letters that Day gave to the taxpayers.[180]

Additionally, the indictment charges that between approximately April 2014 and April 2016, Day prepared false U.S. individual income tax returns for his clients by fabricating and inflating expenses and deductions and/or supplemental loss deductions in order to obtain refunds for his clients in amounts greater than those to which they were entitled. The amounts falsely claimed total $383,773.[181]

Day had his initial appearance in court on February 2, 2017,[182] and his detention was ordered pending trial.[183] Additional legal actions are anticipated.

---

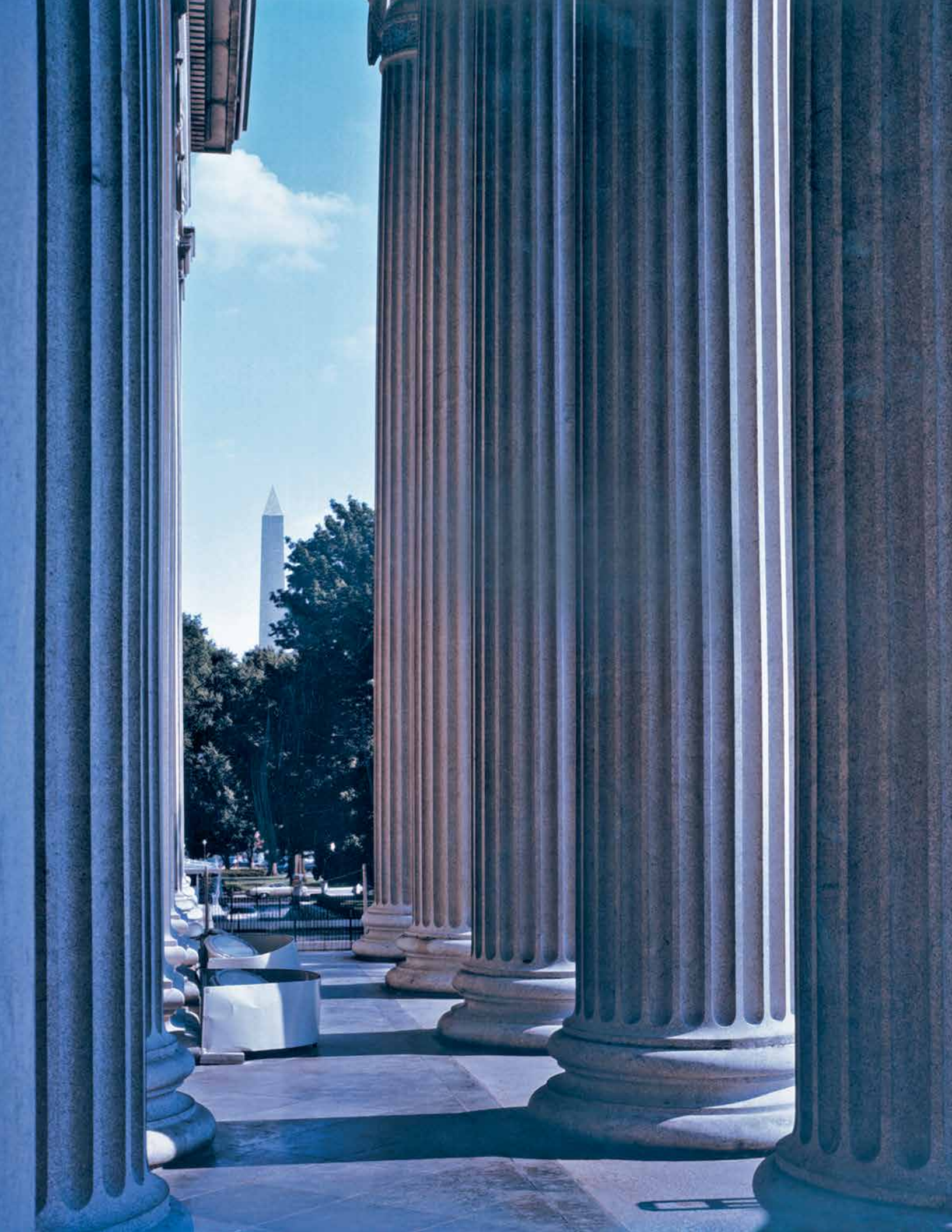
179 Id.

180 Id.

181 Id.

182 D. N.J. Crim. Docket filed Feb. 1, 2017.

183 D. N.J. Order of Detention filed Feb. 2, 2017.



Advancing Oversight of America's Tax System

TIGTA's Office of Inspections and Evaluations (I&E) identifies opportunities for improvement in IRS and TIGTA programs by performing inspections and evaluations that report timely, useful, and reliable information to decision makers and stakeholders.

This function has two primary product lines: inspections and evaluations.

Inspections are intended to:

- Provide factual and analytical information;
- Monitor compliance;
- Measure performance;
- Assess the effectiveness and efficiency of programs and operations;
- Share best practices; and
- Inquire into allegations of waste, fraud, abuse, and mismanagement.

Evaluations are intended to:

- Provide in-depth reviews of specific management issues, policies, or programs;
- Address Governmentwide or multi-agency issues; and
- Develop recommendations to streamline operations, enhance data quality, and minimize inefficient and ineffective procedures.

The following reports highlight some of I&E's most significant activities during this six-month reporting period:

A More Focused Strategy Is Needed to Effectively Address Egregious Employment Tax Crimes

Employment tax noncompliance is a serious crime. When employers fail to account for and deposit employment taxes that they hold in trust on behalf of the Federal Government, they are stealing from the Government. These stolen funds include amounts used to fund important Federal programs, including Social Security and Medicare. As a result of uncollected employment taxes, the Federal Government must use general tax revenues to make whole the Social Security and Medicare trust funds.

The Office of Inspections and Evaluations initiated this project to determine the levels of payroll tax noncompliance identified by the IRS and the extent of civil and criminal enforcement actions taken by the IRS. Employment tax embezzlement is a

felony punishable by up to five years in prison. Employers are required to withhold and timely remit employment (payroll) taxes, which include Federal income taxes, Social Security taxes, and hospital insurance (Medicare) taxes.

TIGTA found that employment tax noncompliance is a growing problem. As of December 2015, 1.4 million employers owed approximately $45.6 billion in unpaid employment taxes, interest, and penalties. The Trust Fund Recovery Penalty (TFRP) is a civil enforcement tool that the IRS Collection function can use to discourage employers from continuing to engage in egregious employment tax noncompliance and provides an additional means of collection enforcement for unpaid employment taxes.

In FY 2015, the IRS assessed the TFRP against approximately 27,000 responsible persons—38 percent fewer than just five years before, as a result of diminished revenue officer resources. In contrast, the number of employers with 20 or more quarters of delinquent employment taxes is steadily growing, more than tripling in the 17-year period. In the case of some tax debtors, assessing the TFRP does not stop the abuse. Although the willful failure to remit employment taxes is a felony, there are fewer than 100 criminal convictions per year. In addition, since the number of actual convictions is so miniscule, there is, in our opinion, likely little deterrent effect.

IRS officials agreed with the development of a focused strategy, but disagreed that the Collection function should expand criteria used to refer cases to CI, citing limited resources and the need to balance several factors involving stakeholders. TIGTA continues to believe that additional egregious cases should be referred for criminal investigation, including cases involving over $1 million and cases with individuals involved in 10 or more companies that failed to remit payroll taxes to the IRS.
Reference No. 2017-IE-R004

Congressional Testimony

On February 15, 2017, Deputy Inspector General for Investigations Timothy P. Camus testified as follows before the Senate Special Committee on Aging to discuss "Stopping Senior Scams: Developments in Financial Fraud Affecting Seniors." All figures given were current as of the date of the testimony.

Since the fall of 2013, much of OI's investigative efforts and resources have been focused on the investigation of a telephone impersonation scam in which more than 1.8 million Americans have reported to TIGTA that they received unsolicited telephone calls from individuals falsely claiming to be IRS or Treasury Department employees and demanding the payment of money for taxes that were not, in fact, due. In addition, the so-called "lottery scam" has reemerged as a significant threat to tax administration.

Since 2013, TIGTA has arrested, indicted, or prosecuted approximately 70 individuals for committing impersonation scams. TIGTA's Office of Investigations has also created an "Advise and Disrupt Strategy" to combat this scam, which has resulted in successfully shutting down 1,056 telephone numbers belonging to impersonation scammers.

TIGTA has made public on the Internet the telephone numbers identified as being associated with the scam, so individuals who have received phone calls can easily look up the numbers online. TIGTA has also set up an auto-dialer "cease and desist" message directed to numbers used by the scammers. In addition, TIGTA ran a public awareness campaign, recording and posting five PSA videos that generated over 71,000 views, and collaborated with private sector companies to help educate the public on this scam.

Lottery scams, which involve scammers calling individuals to offer a prize or lottery money and advising the victims that they must pay a non-existent Federal tax in order to receive the prize, have also been a priority matter at TIGTA. Over the past few years, TIGTA has identified approximately 30 individuals guilty of committing lottery scams.

On March 8, 2017, Assistant Inspector General for Audit Russell Martin testified at a hearing titled "Examining the IRS's Customer Service Challenges," held jointly by the House Committee on Oversight and Government Reform, Subcommittee on Health Care, Benefits and Administrative Rules and Subcommittee on Government Operations.

The annual tax filing season is a critical time for the IRS because it is when most individuals file their income tax returns and contact the IRS. For the 2017 Filing

Season, tax law changes include the continued implementation of the Affordable Care Act and provisions from the PATH Act.

The IRS is becoming increasingly dependent upon technology-based services and the use of external partners, allowing it to focus its limited resources on customer issues that require person-to-person interaction. Taxpayers can receive IRS assistance through technology-based services such as toll-free telephone lines, **IRS.gov**, social media channels, or even the IRS mobile application. This, however, can put taxpayers at risk for fraud and identity theft. Therefore, it is critical that the methods that the IRS uses to authenticate individuals' identities provide a high level of confidence that tax information and services are provided only to individuals who are entitled to receive them.

Most taxpayers continue to use the telephone as their primary method of contacting the IRS about their account. One significant challenge facing the IRS is their Level of Service for over-the-phone contact, which reached 75 percent for the 2017 Filing Season. The IRS also assists taxpayers at their walk-in offices, or TACs. The IRS estimates that the number of taxpayers it will assist at its TACs will continue to decrease, as funding will be channeled away from TACs, and that the number of IRS employees at those offices will continue to be reduced.

Identity-theft tax refund fraud occurs when an individual uses another person's name and Taxpayer Identification Number to file a fraudulent tax return. To further enhance fraud detection, the IRS initiated the W-2 Acceleration Program in PY 2016. This program enables the IRS to receive forms with additional third-party data as early in the filing season as possible, giving the IRS the added ability to exclude legitimate tax returns from identity-theft treatment because the income information matched.

However, some identity-theft victims experienced account errors or long delays in case resolution, and others never received IP PINS. Also, 2.7 million erroneous notices were sent with IP PINS instructing taxpayers not to use their IP PIN if they are claimed as a dependent on a tax return. Almost 1.1 million taxpayers were identified as being victims of employment identity theft but were never notified.

Audit Statistical Reports

Reports With Questioned Costs

TIGTA issued no audit reports with questioned costs during this semiannual reporting period. The phrase "questioned costs" means costs that are questioned because of:

- An alleged violation of a provision of a law, regulation, contract, or other requirement governing the expenditure of funds;
- A finding, at the time of the audit, that such cost is not supported by adequate documentation (an unsupported cost); or
- A finding that an expenditure of funds for the intended purpose is unnecessary or unreasonable.

The phrase "disallowed cost" means a questioned cost that management, in a management decision, has sustained or agreed should not be charged to the Government.

Reports With Questioned Costs

Report Category	Number	Questioned Costs[184] (in thousands)	Unsupported Costs (in thousands)
Reports with no management decision at the beginning of the reporting period	11	$45,543	$0
Reports issued during the reporting period	0	$0	$0
Subtotals (Item 1 plus Item 2)	11	$45,543	$0
Reports for which a management decision was made during the reporting period Value of disallowed costs	0	$0	$0
Value of costs not disallowed	1	$1	$0
Reports with no management decision at the end of the reporting period (Item 3 minus Item 4)	10	$45,542	$0
Reports with no management decision within six months of issuance	10	$45,542	$0

184 "Questioned costs" includes "unsupported costs."

Reports With Recommendations That Funds Be Put to Better Use

TIGTA issued one audit report during this semiannual reporting period with the recommendation that funds be put to better use.[185] The phrase "recommendation that funds be put to better use" means funds could be used more efficiently if management took actions to implement and complete the recommendation, including:

- Reductions in outlays;
- Deobligations of funds from programs or operations;
- Costs not incurred by implementing recommended improvements related to operations;
- Avoidance of unnecessary expenditures noted in pre-award reviews of contract agreements;
- Prevention of erroneous payment of refundable credits, *e.g.*, Earned Income Tax Credit; or
- Any other savings that are specifically identified.

The phrase "management decision" means the evaluation by management of the findings and recommendations included in an audit report, and the issuance of a final decision concerning its response to such findings and recommendations, including actions deemed necessary.

Reports With Recommendations That Funds Be Put to Better Use

Report Category	Number	Amount (in thousands)
1. Reports with no management decision at the beginning of the reporting period	0	$0
2. Reports issued during the reporting period	1	$128,662
3. Subtotals (Item 1 plus Item 2)	**1**	**$128,662**
4. Reports for which a management decision was made during the reporting period		
a. Value of recommendations to which management agreed		
i. Based on proposed management action	1	$128,662
ii. Based on proposed legislative action	0	$0
b. Value of recommendations to which management did not agree	0	$0
5. Reports with no management decision at the end of the reporting period (Item 3 minus Item 4)	**0**	**$0**
6. Reports with no management decision within six months of issuance	0	$0

185 See Appendix II for identification of audit report involved.

Reports With Additional Quantifiable Impact on Tax Administration

In addition to questioned costs and funds put to better use, the Office of Audit has identified measures that demonstrate the value of audit recommendations to tax administration and business operations. These issues are of interest to executives at the IRS and the Department of the Treasury, Members of Congress, and the taxpaying public, and are expressed in quantifiable terms to provide further insight into the value and potential impact of the Office of Audit's products and services. Including this information also promotes adherence to the intent and spirit of the *Government Performance and Results Act.*

Definitions of these additional measures are:

Increased Revenue: Assessment or collection of additional taxes.

Revenue Protection: Ensuring the accuracy of the total tax, penalties, and interest paid to the Federal Government.

Reduction of Burden on Taxpayers: Decreases by individuals or businesses in the need for, frequency of, or time spent on communication, record keeping, preparation, or costs to comply with tax laws, regulations, and IRS policies and procedures.

Taxpayer Rights and Entitlements at Risk: The protection of due process rights granted to taxpayers by law, regulation, or IRS policies and procedures. These rights most commonly arise when filing tax returns, paying delinquent taxes, and examining the accuracy of tax liabilities. The acceptance of claims for and issuance of refunds (entitlements) are also included in this category, such as when taxpayers legitimately assert that they overpaid their taxes.

Taxpayer Privacy and Security: Protection of taxpayer financial and account information (privacy). Processes and programs that provide protection of tax administration, account information, and organizational assets (security).

Inefficient Use of Resources: Value of efficiencies gained from recommendations to reduce cost while maintaining or improving the effectiveness of specific programs; resources saved would be available for other IRS programs. Also, the value of internal control weaknesses that resulted in an unrecoverable expenditure of funds with no tangible or useful benefit in return.

Reliability of Management Information: Ensuring the accuracy, validity, relevance, and integrity of data, including the sources of data and the applications and processing thereof, used by the organization to plan, monitor, and report on its financial and operational activities. This measure will often be expressed as an

absolute value, *i.e.*, without regard to whether a number is positive or negative, of overstatements or understatements of amounts recorded on the organization's documents or systems.

Protection of Resources: Safeguarding human and capital assets, used by or in the custody of the organization, from accidental or malicious injury, theft, destruction, loss, misuse, overpayment, or degradation.

The number of taxpayer accounts and dollar values shown in the following chart were derived from analyses of historical data and are thus considered potential barometers of the impact of audit recommendations. Actual results will vary depending on the timing and extent of management's implementation of the corresponding corrective actions and the number of accounts or subsequent business activities affected as of the dates of implementation. Also, a report may have issues that affect more than one outcome measure category.

Reports With Additional Quantifiable Impact on Tax Administration

Outcome Measure Category	Number of Reports[186]	Number of Taxpayer Accounts	Dollar Value (in thousands)
Increased Revenue	0	0	$0
Revenue Protection	1	324	$9,737
Reduction of Burden on Taxpayers	5	2,780,365	$17,100
Taxpayer Rights and Entitlements at Risk	6	2,044,389	$7,944
Taxpayer Privacy and Security	1	28,200,857	$0
Inefficient Use of Resources	1	0	$3,626
Reliability of Management Information	4	0	$2,568,991
Protection of Resources	0	0	$0

Management did not agree with the outcome measures in the following reports:

- Reduction of Burden on Taxpayers: Reference Number 2017-30-025; and
- Taxpayer Rights and Entitlements at Risk: Reference Number 2017-40-011.

The following reports contained quantifiable impacts other than the number of taxpayer accounts and dollar value:

- Taxpayer Rights and Entitlements at Risk: Reference Number 2017-10-012;
- Innefficient Use of Resources: Reference Number 2017-10-023; and
- Reliability of Information: Reference Numbers 2017-10-005 and 2017-10-012.

186 See Appendix II for identification of audit reports involved

Investigations Statistical Reports[187]

Significant Investigative Achievements

October 1, 2016 – March 31, 2017

Complaints/Allegations Received by TIGTA	
Complaints Against IRS Employees	2,068
Complaints Against Non-Employees	2,891
Total Complaints/Allegations	**4,959**
Status of Complaints/Allegations Received by TIGTA	
Investigations Initiated	886
In Process Within TIGTA[188]	680
Referred to IRS for Action	592
Referred to IRS for Information Only	1,050
Referred to a Non-IRS Entity[189]	2
Closed With No Referral	479
Closed Associated With Prior Investigation	1,093
Closed With All Actions Completed	177
Total Complaints	**4,959**
Investigations Opened and Closed	
Total Investigations Opened	1,426
Total Investigations Closed	1,393
Financial Accomplishments	
Embezzlement/Theft Funds Recovered	0
Contract Fraud and Overpayments Recovered	0
Court Ordered Fines, Penalties, and Restitution	$16,302,422
Out-of-Court Settlements	0
Potentially Compromised by Bribery	0
Tax Liability of Taxpayers Who Threaten and/or Assault IRS Employees	$2,440,797
IRS Assets and Resources Protected Against Malicious Loss	$28,131
Total Financial Accomplishments	**$18,771,350**

187 Includes the new reporting requirements under the Inspector General Empowerment Act (IGEA) of 2016, Pub. L. No. 114-317, 130 Stat. 1595.

188 Complaints for which final determination had not been made at the end of the reporting period.

189 A non-IRS entity includes other law enforcement entities or Federal agencies.

Status of Closed Criminal Investigations

Criminal Referral	Employee	Non-Employee	Total
Referred – Accepted for Prosecution	20	102	**122**
Referred – Declined for Prosecution	227	96	**323**
Referred – Pending Prosecutorial Decision	11	22	**33**
Total Criminal Referrals[190]	**258**	**220**	**478**
No Referral	**360**	**591**	**951**

Criminal Dispositions[191]

Criminal Disposition	Employee	Non-Employee	Total
Guilty	13	29	**42**
Nolo Contendere (no contest)	1	0	**1**
Pretrial Diversion	0	0	**0**
Deferred Prosecution[192]	4	1	**5**
Not Guilty	0	0	**0**
Dismissed	2	1	**3**
Total Criminal Dispositions	**20**	**31**	**51**

Administrative Dispositions on Closed Investigations[193]

Administrative Disposition	Total
Removed / Terminated	**20**
Suspended / Reduction in Grade	**55**
Resigned / Retired / Separated Prior to Adjudication	**67**
Oral or Written Reprimand / Admonishment	**105**
Clearance Letter / Closed, No Action Taken	**114**
Alternative Discipline / Letter With Cautionary Statement / Other	**103**
Non-Employee Actions[194]	**378**
Total Administrative Dispositions	**842**

190 Criminal referrals include both Federal and State dispositions.

191 Final criminal dispositions during the reporting period. These data may pertain to investigations referred criminally in prior reporting periods and do not necessarily relate to the investigations referred criminally in the Status of Closed Criminal Investigations table above.

192 Generally in a deferred prosecution, the defendant accepts responsibility for his/her actions and complies with certain conditions imposed by the court. Upon the defendant's completion of the conditions, the court dismisses the case. If the defendant fails to fully comply, the court reinstates prosecution of the charge.

193 Final administrative dispositions during the reporting period. These data may pertain to investigations referred administratively in prior reporting periods and do not necessarily relate to the investigations closed in the Investigations Opened and Closed table. These data, as reported, reflect a change in the way administrative dispositions were previously categorized.

194 Administrative actions taken by the IRS against non-IRS employees.

Summary of Investigative Reports and Criminal Referrals

Criminal Referral Breakdown (October 1, 2016 – March 31, 2017)	
Number of Investigative Reports Issued	**478**
Referred to DOJ for Criminal Prosecution	461
Referred to State/Local Prosecuting Authorities	17
Number of Indictments and Criminal Informations	**98**
Indictments	86
Criminal Informations	12

The above statistical table was generated as a result of a query of TIGTA OI's case tracking system, Criminal Results Management System (CRIMES).

Interference

During the reporting period there were no attempts by the IRS to interfere with the independence of TIGTA. Additionally, the IRS did not resist, object to oversight activities, or significantly delay access to information.

Instances of Whistleblower Retaliation

During the reporting period there were no investigations regarding whistleblower retaliation.

Closed[195] Investigations Involving Internal Revenue Service Senior Government Employees[196]

Detailed Description of the Facts and Circumstances of the Investigation:	Result:	Disposition:	Criminal Status:	Date Referred:	If Declined, Date of Declination:
A senior Government employee was alleged to have used his/her position to influence a Government contractor to award a subcontract to a specific company.	Substantiated	Separated during investigation	Declined	05/29/15	05/29/15
A senior Government employee was alleged to have engaged in relocation fraud.	Substantiated	Resigned in lieu of termination/ disciplinary action	Declined in lieu of civil proceeding	03/27/14	03/27/14
A senior Government employee was alleged to have engaged in an inappropriate relationship with another employee and making false statements.	Substantiated	Resigned before adjudication	Declined	11/17/16	11/17/16
A senior Government employee was alleged to have made a false statement in response to a congressional inquiry.	Substantiated	Closed without action letter	Declined	11/15/16	11/15/16
A senior Government employee was accused of giving preferential treatment to employees and closing collection activities improperly.	Not Substantiated	Clearance letter	No referral made	N/A	N/A
A senior Government employee was alleged to have overlooked an outside employment request by a subordinate and permitted him/her to use leave to work the unapproved outside employment activity.	Substantiated	Admonished/ reprimanded	No referral made	N/A	N/A
A senior Government employee was alleged to have engaged in an inappropriate relationship with a subordinate. In addition, the employee was also alleged to have threatened the subordinate and provided false statements to investigators.	Substantiated	Suspension	Declined	09/11/14	09/11/14
A senior Government employee reported the loss of his/her laptop, SmartCard, and wireless air card.	Substantiated	Suspension	No referral made	N/A	N/A
A senior Government employee was alleged to have interfered with a criminal investigation being conducted by TIGTA. It was further alleged that this employee may have instructed related witnesses not to be placed under oath by TIGTA.	Substantiated	Resigned before adjudication	Declined	05/23/16	05/23/16
A senior Government employee was alleged to have inaccurately recorded time and attendance records.	Substantiated	Oral/written Counseling	No referral made	N/A	N/A
A senior Government employee was alleged to have discussed a personnel matter in the presence of nonsupervisory employees.	Substantiated	Oral/written Counseling	No referral made	N/A	N/A

195 When TIGTA refers an IRS employee investigation to the IRS, the investigation remains open until all actions are completed, including any penalty imposed upon the employee by the IRS. TIGTA closes an employee investigation after receiving notice from the IRS of the administrative action taken in response to that investigation.

196 For this report, a "senior Government employee" refers to an officer or employee in the Executive branch who occupies a position classified at or above GS–15 of the General Schedule. IGEA § 4(c)(3)(C).

Detailed Description of the Facts and Circumstances of the Investigation:	Result:	Disposition:	Criminal Status:	Date Referred:	If Declined, Date of Declination:
A senior Government employee was alleged to have violated laws, policies, and/or procedures to harass and intimidate another employee.	Not Substantiated	Closed without action letter	No referral made	N/A	N/A
A senior Government employee was alleged to have interfered with a criminal investigation being conducted by TIGTA. It was further alleged that this employee may have instructed related witnesses not to be placed under oath by TIGTA.	Substantiated	Closed without action letter	Declined	05/23/16	05/23/16
A senior Government employee reported a potential compromise of his/her issued laptop when he/she took the laptop outside of the United States on a non-business related trip to perform work.	Substantiated	Other	No referral made	N/A	N/A
A senior Government employee was alleged to have misused his/her Government-issued credit card.	Substantiated	Oral/written counseling	No referral made	N/A	N/A
A senior Government employee reported that his/her Government-issued laptop was stolen out of his/her vehicle.	Substantiated	Other	No referral made	N/A	N/A
A senior Government employee was alleged to have unofficial leave without appropriately reflecting the leave in time and attendance records.	Substantiated	Separated during investigation	Declined	04/18/16	04/18/16
A senior Government employee was arrested for disregarding a traffic control device and operating a motor vehicle under the influence of alcohol or drugs (DUI).	Substantiated	Closed without action letter with cautionary statement	No referral made	N/A	N/A
A senior Government employee was alleged to have received unjust enrichment by receiving a higher compensation for a different locality than where he/she was working.	Substantiated	Other	No referral made	N/A	N/A
A senior Government employee was alleged to have misused his/her Government e-mail account and conducted activities with claims against the Government and other matters affecting the Government.	Substantiated	Admonished/ reprimanded	Declined	04/04/16	04/04/16
A senior Government employee was alleged to have physically assaulted a subordinate.	Not Substantiated	Other	No referral made	N/A	09/28/16
A senior Government employee was alleged to have provided his/her passwords to others, requested that subordinates complete required electronic learning courses on his/her behalf, and committed time and attendance fraud.	Substantiated	Removal/ termination	Declined	08/31/15	08/31/15

Of the 27 investigations, 5 investigations of senior Government employees involved violations of Title 26 of the United States Code (U.S.C.). Due to Federal confidentiality provisions of 26 U.S.C. § 6103, TIGTA is unable to provide additional details regarding these investigations.

Inspections and Evaluations Statistical Reports

Reports With Questioned Costs

TIGTA issued no inspection reports with questioned costs during this semiannual reporting period. The phrase "questioned costs" means costs that are questioned because of:

- An alleged violation of a provision of a law, regulation, contract, or other requirement governing the expenditure of funds;
- A finding, at the time of the inspection, that such cost is not supported by adequate documentation (an unsupported cost); or
- A finding that expenditure of funds for the intended purpose is unnecessary or unreasonable.

The phrase "disallowed cost" means a questioned cost that management, in a management decision, has sustained or agreed should not be charged to the Government.

Reports With Questioned Costs

Report Category	Number	Questioned Costs	Unsupported Costs
1. Reports with no management decision at the beginning of the reporting period	0	$0	$0
2. Reports issued during the reporting period	0	$0	$0
3. **Subtotals (Item 1 plus Item 2)**	**0**	**$0**	**$0**
4. Reports for which a management decision was made during the reporting period a. Value of disallowed costs	0	$0	$0
b. Value of costs not disallowed	0	$0	$0
5. **Reports with no management decision at the end of the reporting period (Item 3 minus Item 4)**	**0**	**$0**	**$0**
6. Reports with no management decision within six months of issuance	0	0	0

Appendix I
Statistical Reports – Other

Reports With Significant Unimplemented Corrective Actions[197]

The Inspector General Empowerment Act of 2016 requires the identification of any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations described in previous semiannual reports for which corrective actions have not been completed. The following list is based on information obtained from the Department of the Treasury's Joint Audit Management Enterprise System.[198],[199]

Reports With Significant Unimplemented Corrective Actions

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2008-20-176	September 2008	09/30/18	THE OFFICE OF RESEARCH, ANALYSIS, AND STATISTICS NEEDS TO ADDRESS COMPUTER SECURITY WEAKNESSES F-1, R-5. Ensure that audit and accountability controls are sufficient by requiring audit logs to be maintained a minimum of six years and to be periodically reviewed by the security officer.
2010-40-055	May 2010	12/15/18	CURRENT PRACTICES ARE PREVENTING A REDUCTION IN THE VOLUME OF UNDELIVERABLE MAIL F-1, R-3. Use hygiene software on any address system to ensure that all outgoing correspondence has an accurate and complete address.
2011-1C-122	September 2011	07/15/17	FINAL INCURRED COST PROPOSAL FOR FISCAL YEAR ENDING APRIL 2, 2004 F-1, R-1. Use the DCAA report in the administration of the contract and determine whether the questioned costs should be recovered. Potential Cost Savings: $28,568,742

197 Acronyms used in this report are defined in the table titled "Acronyms Used Exclusively in Appendices."

198 This summary data does not include reports that are specifically prohibited from disclosure by any provision of law, such as 26 U.S.C. § 6103 protecting tax returns and return information, or that are specifically required by Executive order to be protected from disclosure in the interest of national defense or national security or in the conduct of foreign affairs.

199 The Office of Audit has previously designated three reports with unimplemented recommendations as "Sensitive But Unclassified (SBU)." These SBU reports concern physical security of IRS facilities or subject matter that might create a risk of circumvention of the law if publicly released. There are no potential cost savings associated with any unimplemented recommendations from these three reports.

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2012-1C-003	December 2011	04/15/17	CONTRACTOR'S FISCAL YEAR 2007 INCURRED COST PROPOSAL F-1, R-1. Use the DCAA report in the administration of the contract and determine whether the questioned costs should be recovered. Potential Cost Savings: $15,732
2012-1C-032	March 2012	09/15/17	FINAL INCURRED COST PROPOSAL FOR FISCAL YEAR ENDING APRIL 1, 2005 F-1, R-1. Use the DCAA report in the administration of the contract and determine whether the questioned costs should be recovered. Potential Cost Savings: $7,416,602
2012-1C-079	August 2012	08/07/17	FISCAL YEAR 2011 COMPLIANCE WITH REQUIREMENTS OF OFFICE OF MANAGEMENT AND BUDGET CIRCULAR A-133 APPLICABLE TO RESEARCH AND DEVELOPMENT F-1, R-1. Use the DCAA report in administering and closing out contracts. Potential Cost Savings: $1,477,659
2013-1C-001	March 2013	03/18/18	INDEPENDENT AUDIT OF THE CONTRACTOR'S CIVIL INFORMATION TECHNOLOGY FISCAL YEAR ENDED MARCH 31, 2006, FINAL INCURRED COST PROPOSAL F-1, R-1. Use the DCAA report in administering and closing out contracts. Potential Cost Savings: $327,845
2013-20-025	June 2013	11/15/17 11/15/17 11/15/17	DESKTOP AND LAPTOP SOFTWARE LICENSE MANAGEMENT IS NOT BEING ADEQUATELY PERFORMED F-2, R-2. To help ensure that the User and Network Services organization has processes for using software license tools that adhere to Federal requirements and recommended best practices, implement a specialized software license tool designed to discover, track, and manage software license deployment and usage. F-3, R-1. To help ensure that the User and Network Services organization has processes for software license inventories that adhere to Federal requirements and recommended best practices, the Chief Technology Officer should develop an inventory of software licensing data and maintain the inventory with a specialized software license tool designed to discover, track, and manage software license deployment and usage. F-3, R-2. To help ensure that the User and Network Services organization has processes for software license inventories that adhere to Federal requirements and recommended best practices, maintain data in the inventory that the IRS can use to more effectively review software licensing agreements, purchases, deployment, usage, and other related aspects of licensing to identify additional savings in software spending.
2013-20-089	September 2013	06/15/17	WEAKNESSES IN ASSET MANAGEMENT CONTROLS LEAVE INFORMATION TECHNOLOGY ASSETS VULNERABLE TO LOSS F-2, R-2. Ensure that KISAM-AM information is timely updated and maintained.

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2013-20-107	September 2013		FULL COMPLIANCE WITH TRUSTED INTERNET CONNECTION REQUIREMENTS IS PROGRESSING; HOWEVER, IMPROVEMENTS WOULD STRENGTHEN SECURITY
		09/25/16	F-1, R-3. Ensure that the IRS obtains Top Secret Sensitive Compartmented Information clearances for IRS operational employees who can receive and react to classified information on a 24/7 basis.
		09/25/16	F-1, R-4. Ensure that the IRS completes implementation of the Sensitive Compartmented Information Facilities at TIC management locations.
2014-1C-018	March 2014		INDEPENDENT AUDIT OF THE CONTRACTOR'S INCURRRED COST PROPOSAL FOR FISCAL YEAR ENDING MARCH 30, 2007
		12/19/18	F-1, R-1. Use the DCAA report in administering and closing out contracts.
			Potential Cost Savings: $6,470,339
2014-1C-019	May 2014		INDEPENDENT AUDIT OF THE CONTRACTOR'S ASSET MANAGEMENT'S INCURRED COSTS FOR FISCAL YEAR ENDED DECEMBER 31, 2005
		05/29/19	F-1, R-1. Use the DCAA report in administering and closing out contracts.
			Potential Cost Savings: $8,431
2014-10-033	June 2014		THE TAXPAYER ADVOCATE SERVICE CAN IMPROVE THE PROCESSING OF SYSTEMIC BURDEN CASES
		09/30/17	F-1, R-1. Reissue guidance to explain the requirement to only contact authorized representatives when applicable, and emphasize this in future training.
		09/30/17	F-1, R-3. Review the results of sample findings and incorporate lessons learned into future training.
2014-20-083	September 2014		THE INTERNAL REVENUE SERVICE SHOULD IMPLEMENT AN EFFICIENT INTERNAL INFORMATION SECURITY CONTINUOUS MONITORING PROGRAM THAT MEETS ITS SECURITY NEEDS
		08/15/17	F-1, R-1. Select and implement an integrated dashboard of the security scanning tools to allow stakeholder and decision makers to make well informed risk based decisions.
2014-40-084	September 2014		A SERVICE-WIDE STRATEGY IS NEEDED TO INCREASE BUSINESS TAX RETURN ELECTRONIC FILING
		12/15/20	F-2, R-1. Develop a less burdensome electronic signature process for businesses e-filing employment tax returns using the Modernized e-File system.
2014-20-085	September 2014		INCREASED SUPPORT IS NEEDED TO ENSURE THE EFFECTIVENESS OF THE FINAL INTEGRATION TEST
		10/15/17	F-3, R-1. To ensure that the FIT program's environment simulates the filing season environment as closely as possible, implement the environment comparison and synchronization process between the FIT program's environment and the filing season environment.

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2015-10-011	March 2015		EXISTING PROCUREMENT PRACTICES ALLOWED CORPORATIONS WITH FEDERAL TAX DEBT TO OBTAIN CONTRACT AWARDS
		05/31/17	F-1, R-4. Develop procedures to determine what constitutes an unpaid Federal tax liability that is consistent with the definition outlined in the Consolidated Appropriations Act of 2012. Once a determination of what constitutes an unpaid Federal tax liability has been developed, provide such information to the contracting officers to use in the conduct of comprehensive tax checks and to the Department of the Treasury Suspension and Debarment official for the purpose of making contract award decisions that are in compliance with the Act.
2015-1C-039	July 2015		PROPOSED AMOUNTS ON UNSETTLED FLEXIBLY PRICED CONTRACTS FOR FISCAL YEAR 2008
		02/19/18	F-1, R-1. Use the DCAA report in administering and closing out contracts.
			Potential Cost Savings: $420,257
2015-1C-040	July 2015		PROPOSED AMOUNTS ON UNSETTLED FLEXIBLY PRICED CONTRACTS FOR FISCAL YEAR 2008
		02/11/19	F-1, R-1. Use the DCAA report in administering and closing out contracts.
			Potential Cost Savings: $461,653
2015-30-052	July 2015		IMPROVEMENT IS NEEDED IN COMPLIANCE EFFORTS TO IDENTIFY UNSUPPORTED CLAIMS FOR FOREIGN TAX CREDITS
		09/29/17	F-2, R-1. Develop a compliance strategy to address the risks identified with the FTC, including the issues of taxpayers receiving both the credit and the deduction for the same foreign tax payments, and taxpayers claiming the FTC without the proper third-party information return documentation.
			Potential Cost Savings: $40,000,000
2015-30-056	July 2015		IMPROVEMENTS ARE NEEDED TO VERIFY TAXPAYER CLAIMS FOR EXEMPTION FROM UNITED STATES SOCIAL SECURITY TAXES UNDER TOTALIZATION AGREEMENTS
		09/29/17	F-1, R-1. Use existing procedures to work with the SSA on establishing a process to periodically acquire Certificate of Coverage data.
		09/29/17	F-1, R-2. Coordinate with the SSA Competent Authority to request data from countries with which the United States has Totalization Agreements, related to foreign social security taxes paid by American citizens, resident aliens, or withheld and paid by American employers, that would help the IRS ensure compliance with the United States Social Security tax laws.
		04/15/17	F-1, R-3. Use the data obtained from the other Totalization Agreement countries and the SSA to identify noncompliance with payment of United States Social Security and Medicare taxes.
			Potential Cost Savings: $105,985,023

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2016-40-008	December 2015		CONTINUED REFINEMENT OF THE RETURN REVIEW PROGRAM IDENTITY THEFT DETECTION MODELS IS NEEDED TO INCREASE DETECTION
		On Hold	F-2, R-2. Ensure that tax examiners reverse the fraudulent tax return data entries from the taxpayer's account and place an identity theft indicator on the taxpayer's account for an undelivered check when the taxpayer has not satisfactorily resolved the issue after 30 calendar days.
		06/15/17	F-2, R-3. Develop processes and procedures to place an identity theft indicator and remove the fraudulent tax return data for those taxpayer accounts for which a paper refund check is cancelled because it remains uncashed after 14 months.
2016-10-014	January 2016		INDEPENDENT ATTESTATION REVIEW OF THE INTERNAL REVENUE SERVICE'S FISCAL YEAR 2015 ANNUAL ACCOUNTING OF DRUG CONTROL FUNDS AND RELATED PERFORMANCE
		09/15/17	F-1, R-1. Develop future performance goals that are consistent with the IRS's documented methodology and clearly explained in the Detailed Accounting Submission and Performance Summary Report.
2016-20-019	February 2016		MANAGEMENT OVERSIGHT OF THE TIER II ENVIRONMENT BACKUP AND RESTORATION PROCESS NEEDS IMPROVEMENT
		04/15/17	F-2, R-2. Incorporate the IRS software modernization initiative, Infrastructure Currency, into written policies and guidelines for keeping software current. This policy should ensure that software is supported and compatible.
2016-1C-026	April 2016		SUPPLEMENT AUDIT OF THE CONTRACTOR FEDERAL PROPOSED AMOUNTS ON UNSETTLED FLEXIBLY PRICED CONTRACTS FOR FISCAL YEAR 2009
		04/15/21	F-1, R-1. Use the DCAA report in administering and closing out contracts.
			Potential Cost Savings: $374,821
2016-40-028	March 2016		REVISING TAX DEBT IDENTIFICATION PROGRAMMING AND CORRECTING PROCEDURAL ERRORS COULD IMPROVE THE TAX REFUND OFFSET PROGRAM
		On Hold	F-1, R-1. Revise identification processes to include sole proprietor information from Form SS-4 to identify individual tax refunds to offset to business tax debt.
		On Hold	F-2, R-4. Revise computer programming to ensure that credit elects are offset to any associated tax debt on the Non-Master File.
		On Hold	F-3, R-1. Revise computer programming to use the LLC indicator on the business tax account to ensure that individual tax refunds are not offset to the associated LLC's business tax debt.
		10/15/17	F-3, R-2. Identify and transfer the incorrect offsets totaling $780,474 from the 502 LLC accounts back to the individual taxpayer accounts. In addition, identify other accounts with incorrect offsets subsequent to the time frame of TIGTA's TY 2013 analysis until programming is corrected and transfer incorrectly offset refunds back to the individual taxpayer accounts.
2016-30-030	June 2016		IMPROVEMENTS ARE NEEDED IN OFFSHORE VOLUNTARY DISCLOSURE COMPLIANCE AND PROCESSING EFFORTS
		On Hold	F-2, R-2. Establish one mailing address for taxpayers to use for submitting their offshore voluntary disclosure requests and related documentation.

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2016-30-031	April 2016		OPPORTUNITIES EXIST TO IDENTIFY AND EXAMINE INDIVIDUAL TAXPAYERS WHO DEDUCT POTENTIAL HOBBY LOSSESS TO OFFSET OTHER INCOME
		09/15/17	F-2, R-1. Emphasize the importance of required filing checks in the preliminary determination of whether to pursue an I.R.C. § 183 issue and provide tools to assist examiners in documenting their conclusion.
2016-30-032	May 2016		IMPROVEMENTS ARE NECESSARY TO ENSURE THAT INDIVIDUAL AMENDED RETURNS WITH CLAIMS FOR REFUNDS AND ABATEMENTS OF TAXES ARE PROPERLY REVIEWED
		06/15/17	F-1, R-3. Establish a process for group managers to document their decisions to survey claims, which would include documenting the results of their risk analyses.
		06/15/17	F-2, R-1. Issue guidance to field examiners and group managers that stresses the importance of obtaining adequate documentation to support the validity of claims as well as their responsibility to review and document LUQ items considered during audits.
		06/15/17	F-2, R-3. Take steps to ensure that potential underreported income and financial status issues on returns with claims for refunds or abatements of taxes are adequately addressed.
2016-43-033	March 2016		AFFORDABLE CARE ACT: INTERNAL REVENUE SERVICE VERIFICATION OF PREMIUM TAX CREDIT CLAIMS DURING THE 2015 FILING SEASON
		On Hold	F-2, R-1. Modify the Income and Family Size Verification processes to use the most current data available at the time a request is received from an Exchange when determining if a taxpayer has reconciled Advance Premium Tax Credits received in the prior calendar year.
2016-10-039	July 2016		TELEWORK QUALIFICATION REQUIREMENTS ARE GENERALLY BEING MET, BUT PROGRAM IMPROVEMENTS ARE NEEDED
		06/30/17	F-1, R-2. Clarify the rules associated with misconduct by clearly defining issues that warrant suspension and discontinuance of telework privileges.
		06/30/17	F-1, R-3. Develop procedures for identifying teleworking employees who have been disciplined for conduct that negatively impacts the Telework Program.
2016-30-047	July 2016		FISCAL YEAR 2016 STATUTORY REVIEW OF COMPLIANCE WITH NOTICE OF FEDERAL TAX LIEN DUE PROCESS PROCEDURES
		07/15/17	F-1, R-1. Determine if programming changes are viable for the systemic upload and use of the secondary taxpayer's last known address for mailing lien notices for NFTLs with joint liabilities. Also, revise applicable IRM sections to require employees requesting an NFTL involving joint liability to research IDRS for the last known address of the secondary spouse.
2016-10-048	July 2016		THE INTERNAL REVENUE SERVICE HAS A PROCESS TO RESPOND TO WORKPLACE INJURIES, BUT SOME IMPROVEMENTS COULD BE MADE
		01/15/18	F-1, R-2. Evaluate the findings from the IRS facilities TIGTA visited to determine whether a revision to the IRM is needed to reinforce the requirement that safety officers perform and document safety investigations after an employee has been injured.
		07/15/17	F-1, R-3. Identify a way to notify safety officers when an employee has filed a workers' compensation claim through an e-mail alert or other electronic means.
		07/15/17	F-2, R-1. Ensure that all applicable safety inspections are performed annually as required. This should include tracking when inspections are required, ensuring that inspections are reviewed for hazards, and documenting dates on the GDI.

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2016-10-049	July 2016		SIGNIFICANT IMPROVEMENTS ARE NEEDED IN THE CONTRACTOR TAX CHECK PROCESS
		04/15/17	F-1, R-2. Ensure that Office of Procurement tax check policies and procedures provide COs the ability to communicate tax check results, which indicate tax debt, to the affected contractors and obtain their consent to use the tax information for purposes of determining contractor responsibility and eligibility for award.
		04/15/17	F-1, R-3. Ensure procurement policies for responsibility determination implement the requirements of Federal appropriations law. Further, provide mandatory training to COs to strengthen their understanding of the proper procedure for requesting a tax check, how to use the tax check results to determine contractor award eligibility, the process for communicating the results to the contractor (as appropriate), and how to properly document the contract award decisions in their contract files.
		04/15/17	F-1, R-4. Ensure that tax checks are requested on all solicitations, regardless of award amount, so COs do not inadvertently violate the conditions placed upon the expenditure of appropriated funds.
2016-30-052	July 2016		FISCAL YEAR 2016 STATUTORY REVIEW OF COMPLIANCE WITH LEGAL GUIDELINES WHEN ISSUING LEVIES
		09/15/17	F-1, R-1. Monitor manual and systemic ACS levies with additional assessments until it is determined that all systemic programming fixes are working.
		05/15/17	F-2, R-2. Monitor ICS systemic levies with additional assessments until it is determined that all systemic programming fixes are working.
2016-IE-R008	August 2016		THE OFFER IN COMPROMISE PUBLIC INSPECTION FILE ACTIVITY DOES NOT HAVE ADEQUATE MANAGEMENT OVERSIGHT OR CONTROLS:
		04/15/17	F-1, R-1. Develop processes to convert paper-based offer in compromise public inspection files to an electronic format to better manage the retrieval, movement, retention, and destruction of files. In addition, consider the feasibility of creating an online public website that provides access to all accepted offer in compromise files while ensuring that sensitive information is being properly redacted.
2016-10-056	August 2016		IMPROVEMENTS IN CONTROLS ARE NEEDED FOR LAPTOP COMPUTERS RECOVERED WHEN EMPLOYEES SEPARATE
		09/30/17	F-1, R-2. Develop procedures to reconcile and resolve discrepancies between clearance module records and IT office inventory records when employees separate.
2016-10-057	August 2016		IMPROVED CONTROLS ARE NEEDED TO ACCOUNT FOR THE ISSUANCE AND RETURN OF CONTRACTOR EMPLOYEE LAPTOP COMPUTERS
		09/15/17	F-1, R-1. Strengthen management oversight by updating appropriate checklists (or the appropriate contract administration process) and conduct training to provide reasonable assurance that barcodes are documented in contract administration documentation for the issuance of laptop computers to contractor employees and the return of laptop computers from contractor employees.
		09/15/17	F-1, R-2. Develop a process to review and compare contract administration documentation to computer inventory records to provide reasonable assurance that barcodes are documented correctly in contract administration files for the issuance and return of laptop computers to contractor employees.

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2016-30-059	August 2016		THE WHISTLEBLOWER PROGRAM HELPS IDENTIFY TAX NONCOMPLIANCE; HOWEVER, IMPROVEMENTS ARE NEEDED TO ENSURE THAT CLAIMS ARE PROCESSED APPROPRIATELY AND EXPEDITIOUSLY
		04/15/17	F-1, R-1. Ensure that any I.R.C. § 7623(a) claims that are sent to the SMEs are subject to the debriefing requirement in the August 20, 2014, memorandum from the IRS Deputy Commissioner for Services and Enforcement.
		07/15/17	F-1, R-2. Verify that operating division SMEs are following the requirement for debriefing whistleblowers and provide results to operating divisions for possible improvements.
		07/15/17	F-2, R-1. Ensure that management monitoring reports for the Whistleblower Program include data to determine if processing targets are being achieved, e.g., cycle time for claims at key processing steps.
		09/30/17	F-4, R-1. Implement the Balanced Performance Measurement System for the Whistleblower Program.
		04/15/17	F-4, R-2. Develop a structured quality review process for the Whistleblower Program.
		04/15/17	F-4, R-3. Establish systemic computer validation checks on E-TRAK to minimize the initial entry of inaccurate data, and establish methods to identify and correct inaccurate entries.
		09/30/17	F-4, R-5. Incorporate key guidance into the IRM to explain Whistleblower Program operations and update when necessary.
		07/15/17	F-5, R-1. Implement a process to quickly identify and reject claims submitted by all types of ineligible whistleblowers.
2016-30-060	August 2016	07/15/17	FISCAL YEAR 2016 STATUTORY REVIEW OF DISCLOSURE OF COLLECTION ACTIVITIES ON JOINT RETURNS
			F-1, R-2. Incorporate into existing training how to handle oral and written requests received under I.R.C. Sections 6103(e)(7) and (e)(8) for all IRS employees who would receive these types of requests while interacting with taxpayers on the telephone, as appropriate.
2016-40-069	August 2016	04/15/17	ACTIONS ARE NEEDED TO BETTER IDENTIFY AND ADDRESS INDIVIDUALS WHO FILE TAX RETURNS USING FRIVOLOUS ARGUMENTS
			F-2, R-1. Ensure that all IRS employees who are responsible for identifying tax returns claiming potentially frivolous arguments complete frivolous return training annually.

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2016-30-070	September 2016		EXAMINATION COLLECTIBILITY PROCEDURES NEED TO BE CLARIFIED AND APPLIED CONSISTENTLY
		11/15/17	F-1, R-1. Revise the IRM to provide clear instructions on documenting collectability determinations, including examples of when cases should be given consideration for being surveyed and not given consideration for being surveyed due to collectability considerations.
			Potential Cost Savings: $75,558,865
		11/15/17	F-1, R-2. Provide training to examiners on collectability determinations.
		11/15/17	F-1, R-3. Consider tracking returns that are surveyed due to collectability.
		11/15/17	F-2, R-1. Provide training to examiners on the need to coordinate with the Collection function.
		11/15/17	F-2, R-2. Revise the IRM to be consistent about when the examiner should contact the Collection function.
		11/15/17	F-2, R-3. Consider the feasibility of adding a Master File indicator to alert the Collection function when a taxpayer was unable to be contacted or located during an examination.
		11/15/17	F-3, R-1. Use available resources, such as the Enforcement Revenue Information System, to measure and track collectability as it relates to examination assessments and the goal of decreasing the ARDI and increasing the quality of assessments.
2016-20-075	September 2016		INFORMATION TECHNOLOGY: SHAREPOINT CONTROLS NEED IMPROVEMENT TO MITIGATE RISKS AND TO ENSURE THAT POSSIBLE DUPLICATE COSTS ARE AVOIDED
		04/15/17	F-1, R-2. Ensure that SharePoint site collections containing PII or SBU data have approved PCLIAs.
		04/15/17	F-1, R-3. Ensure that an SA&A considers the SharePoint product, sites, and data within the appropriate authorization boundary and assesses key security controls.
		06/15/17	F-1, R-4. Coordinate with the respective business unit commissioners to ensure that the SharePoint site collection owners and administrators enable audit trails of key user activities on their sites and that they review audit trails on a regular basis.
		06/15/17	F-1, R-5. Coordinate with the respective business unit commissioners to ensure that SharePoint site owners and administrators perform quarterly reviews of user accesses in order to ensure that only authorized users with a business need have access to perform their assigned responsibilities.
		06/15/17	F-1, R-6. Coordinate with the respective business unit commissioners to ensure that the SharePoint site owners and administrators efficiently manage user permissions by consistently assigning users and appropriate permissions to groups.
		06/15/17	F-1, R-7. Coordinate with the respective business unit commissioners to ensure that the SharePoint governance structure is enhanced to provide enterprise adherence to SharePoint security and content management policies.
		05/15/17	F-1, R-8. Ensure that the draft SharePoint Information Technology Contingency Plan, including a Business Impact Analysis, is finalized and approved by management.
		06/15/17	F-2, R-1. Ensure that a feasibility analysis is conducted regarding use of the Treasury Enterprise Content Management environment, including an assessment of functionality, security, risks, costs, and benefits.
		06/15/17	F-2, R-2. Ensure that the IRS's decision regarding use of the Treasury Enterprise Content Management environment is based on the conclusions of the above feasibility analysis.

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2016-40-078	September 2016		DUE TO THE LACK OF ENFORCEMENT, TAXPAYERS ARE AVOIDING BILLIONS OF DOLLARS IN BACKUP WITHHOLDING
		09/15/17	F-1, R-1. Establish a Service-wide information returns backup withholding enforcement strategy. This should include specific time frames and actions that will be taken to identify and enforce payer noncompliance with backup withholding provisions.
		11/15/17	F-2, R-1. Evaluate and document the criteria used to exclude information returns with missing or incorrect TINs from payer notification.
		11/15/17	F-3, R-1. Update payer identification and notification processes to include Forms 1099-G with missing or incorrect payee TINs.
		03/15/18	F-3, R-2. Update all applicable publications, instructions, and website information to include Forms 1099-G as the payments relate to backup withholding provisions.
2016-20-080	September 2016		REVIEW OF THE ENTERPRISE E-MAIL SYSTEM ACQUISITION
		07/15/17	F-1, R-1. Ensure that IRM 2.21 and IRM 2.16.1 requirements regarding the Commercial Off-the-Shelf Path or the Managed Services Path are followed prior to the subscription requisition process and throughout the subscription project development life cycle for new subscription or managed services procurements.
2016-20-082	September 2016		IMPROVEMENTS ARE NEEDED TO STRENGTHEN ELECTRONIC AUTHENTICATION PROCESS CONTROLS
		04/15/17	F-2, R-2. Ensure that the IRS provides security specialists with adequate tools and related training to perform analysis as described in audit plans.
		12/15/17	F-4, R-1. Compile periodic summary data of eAuthentication volume and unusual activity trigger event transactions, so that data can be compared over time to identify trends or outliers.
		06/15/17	F-4, R-2. Ensure that the eAuthentication audit trail includes an EventID that indicates which target application the user intended to access after authenticating.
2016-30-083	September 2016		AS THE USE OF VIRTUAL CURRENCIES IN TAXABLE TRANSACTIONS BECOMES MORE COMMON, ADDITIONAL ACTIONS ARE NEEDED TO ENSURE TAXPAYER COMPLIANCE
		09/30/17	F-1, R-1. Develop a coordinated virtual currency strategy that includes outcome goals, a description of how the agency intends to achieve those goals, and an action plan with a timeline for implementation. In addition, the strategy should use the tools available to the IRS and identify how the IRS is going to meet its Bank Secrecy Act, criminal investigation, and tax enforcement obligations as related to virtual currencies as well as identify how actions will be monitored and the methodologies used to measure the actions taken.

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2016-30-085	September 2016		IMPROVEMENTS TO THE NONFILER PROGRAM COULD HELP THE INTERNAL REVENUE SERVICE MORE EFFECTIVELY ADDRESS ADDITIONAL NONFILERS OWING BILLIONS OF DOLLARS IN TAXES
		10/15/17	F-1, R-4. Analyze the population of TY 2013 HINFs with expired extensions identified as not having filed a tax return and notify those taxpayers of the requirement to file the TY 2013 tax return. If resources do not allow for the notification of the entire population, document the analysis performed to determine the percentage or number of TY 2013 HINFs with expired extensions that should be notified.
			Potential Cost Savings: $2,700,000,000
		10/15/17	F-2, R-1. Develop a strategy for evaluating and improving the effectiveness of the delinquency notice, which may include tracking the reasons for taxpayer inquiries at IRS call sites.
		10/15/17	F-2, R-2. Revise the nonfiler strategy to include specific action items aimed at increasing the number of nonfilers who are contacted and the nonfiler response rate. Action items should focus on increasing automation and addressing areas of taxpayer confusion in an effort to limit any additional burden on current resources in the Compliance Services Collection Operations function.
2016-30-087	September 2016		FISCAL YEAR 2016 STATUTORY AUDIT OF COMPLIANCE WITH LEGAL GUIDELINES PROHIBITING THE USE OF ILLEGAL TAX PROTESTER AND SIMILAR DESIGNATIONS
		11/15/17	F-1, R-1. Emphasize to all examination employees the importance of compliance with the RRA 98 § 3707 and reinforce that taxpayers are not to be referred to as Illegal Tax Protestors or any other similar designations. This may include, but is not limited to, updating examination procedures, issuing a memorandum, or adding a module to an existing training course.
2016-30-089	September 2016		THE LARGE BUSINESS AND INTERNATIONAL DIVISION'S STRATEGIC SHIFT TO ISSUE-FOCUSED EXAMINATIONS WOULD BENEFIT FROM RELIABLE INFORMATION ON COMPLIANCE RESULTS
		09/15/17	F-2, R-1. Develop and implement plans to streamline the UIL codes available to examiners, provide additional guidance for the appropriate use of UIL codes, and include UIL code accuracy in program and evaluative quality reviews.

Reference Number	Issued	Projected Completion Date	Report Title and Recommendation Summary (F = Finding No., R = Recommendation No.)
2016-30-090	September 2016		BARRIERS EXIST TO PROPERLY EVALUATING TRANSFER PRICING ISSUES
		10/15/17	F-1, R-1. Ensure that employees follow the Roadmap and include this as an attribute of the quality review process.
		10/15/17	F-1, R-2. Ensure that taxpayers undergoing examinations with a transfer pricing issue have a clear understanding of the Roadmap. This should include providing them a copy of the Roadmap prior to the beginning of the examination engagement and requiring employees to be consistent in its use.
		09/15/18	F-2, R-1. Ensure that TPP employees have full access to the SRS and that they work collaboratively with the IBC function to ensure that transfer pricing issues are consistently identified and directed for specialized review.
		10/15/17	F-2, R-3. Ensure that adequate transfer pricing training is provided. The LB&I Division should require mandatory transfer pricing specific training for TPP and IBC function employees and managers. The LB&I and SB/SE Divisions should ensure that LB&I (Domestic) and SB/SE Divisions' Examination function employees and managers with potential exposure to transfer pricing issues be adequately trained to identify, refer (as necessary), and work transfer pricing issues appropriately. Detailed training plans should be implemented and include documentation and tracking of all employees' successful completion of the mandatory training.
		09/15/18	F-3, R-1. Develop a comprehensive transfer pricing strategy that includes outcome-related strategic goals, a description of how the LB&I Division intends to achieve those goals, and an action plan with a timeline for implementation. This strategy should measure the success and productivity of the examinations of transfer pricing issues. This should include, but is not limited to, the amount of the examination adjustments and the taxes ultimately assessed.
2016-20-093	September 2016		UPDATING COMPUTER ROOM AND TAPE LIBRARY PHYSICAL ACCESS CONTROLS AT THE COMPUTING CENTERS WILL SIGNIFICANTLY IMPROVE SECURITY
		08/15/17	F-1, R-2. Implement a FIPS 201 compliant two-factor authentication for the computer rooms and tape library at the ECC in Memphis.

Other Statistical Reports

The Inspector General Empowerment Act of 2016 requires Inspectors General to address the following issues for the Offices of Audit and Inspections and Evaluations:[200]

Issue	Result for TIGTA
Interference/Access to Information Report any attempt to interfere with the independence of TIGTA, including: budget constraints designed to limit the capabilities of TIGTA; and incidents of resistance or objection to oversight activities of TIGTA. Report restricted or significantly delayed access to information, including the justification of the establishment for such action.	As of March 31, 2017, there were no attempts to interfere with the independence of TIGTA or any instances of restricted or significantly delayed access to information.
Disputed Recommendations Provide information on significant management decisions in response to recommendations with which the Inspector General disagrees.	As of March 31, 2017, there were no instances in which significant recommendations were disputed.
Revised Management Decisions Provide a description and explanation of the reasons for any significant revised management decisions made during the reporting period.	As of March 31, 2017, there were no significant revised management decisions.
Reports Issued in the Prior Reporting Period With No Management Response Provide a summary of each report issued before the beginning of the current reporting period for which no management response was received within 60 days of the report issuance date.	As of March 31, 2017, there were no prior reports for which management's response was not received within 60 days of issuance.
Disclosure Provide detailed descriptions of the circumstances of each inspection, evaluation, and audit that was closed by the agency and was not disclosed to the public.	As of March 31, 2017, there were no reports that had been closed and were not disclosed to the public.
Review of Legislation and Regulations Review existing and proposed legislation and regulations, and make recommendations concerning the impact of such legislation or regulations.	TIGTA's Office of Chief Counsel reviewed 164 proposed regulations and legislative requests during this reporting period.

200 Results listed are for this reporting period only.

Appendix II
Audit Products

October 1, 2016 - March 31, 2017

Audit Products	
Reference Number	**Report Title**
October 2016	
2017-1C-001	Report of the Contractor's Corporate Proposed Allocation Amounts on Unsettled Flexibly Priced Contracts for Fiscal Years 2011 and 2012
2017-1C-003	Audit of the Contractor's North American Public Sector Proposed Allocation Amounts on Unsettled Flexibly Priced Contracts for Fiscal Years 2011 and 2012
2017-30-009	Important Improvements Have Been Made in the Offer in Compromise Process; However, Additional Efficiencies Can Be Gained (Taxpayer Burden: 12,754 taxpayer accounts impacted)
2017-1C-002	Audit of the Contractor's Proposed Amounts on Unsettled Flexibly Priced Contracts for Fiscal Years 2009 and 2010
2017-30-010	Employees Sometimes Did Not Adhere to E-mail Policies Which Increased the Risk of Improper Disclosure of Taxpayer Information (Taxpayer Privacy and Security: 28,200,857 taxpayer accounts impacted)
2017-20-004	Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners
November 2016	
2017-40-011	Actions Can Be Taken to Improve Processes of a Newly Developed Program That Enables Victims of Identity Theft to Request Copies of Fraudulent Tax Returns (Taxpayer Rights and Entitlements: 498 taxpayer accounts impacted)
2017-10-005	Improvements Are Needed in the Taxpayer Advocate Service Process to Implement Recommended Corrective Actions (Reliability of Information: 13 corrective actions impacted)
2017-1C-006	Report of the Contractor's Corporate Proposed Allocation Amounts on Unsettled Flexibly Priced Contracts for Fiscal Years 2010 Through 2012
December 2016	
2017-40-013	Analysis of Resources Allocated to Taxpayer Services
January 2017	
2017-10-012	The Office of Chief Counsel Accurately Administered User Fees but Could Improve Its User Fee Refund Process (Taxpayer Rights and Entitlements: $57,925 impacting 24 taxpayers and 23 cases; Reliability of Information: 226 cases files impacted)
2017-1C-007	Report of the Contractor's Defense Home Office's Proposed Amounts on Unsettled Flexibly Priced Contracts for Fiscal Years 2009 and 2010
2017-1C-008	Report of the Contractor's Home Office Proposed Allocation Amounts on Unsettled Flexibly Priced Contracts for Fiscal Years 2011 and 2012
2017-10-015	Review of the Internal Revenue Service's Purchase Card Violations Report and the Status of Government Charge Card Recommendations
2017-10-016	Independent Attestation Review of the Internal Revenue Service's Fiscal Year 2016 Annual Accounting of Drug Control Funds and Related Performance
2017-40-014	Results of the 2016 Filing Season (Revenue Protection: $9,737,049 impacting 324 taxpayer accounts; Taxpayer Burden: 126 Taxpayer accounts impacted; Taxpayer Rights and Entitlements: $1,218,266 impacting 707 taxpayer accounts)

February 2017	
2017-40-017	Efforts Continue to Result in Improved Identification of Fraudulent Tax Returns Involving Identity Theft; However, Accuracy of Measures Needs Improvement (Reliability of Information: $2,538,100,000 overstated revenue)
2017-43-021	Affordable Care Act: Analysis of Tax Year 2014 Nonfilers Who Received Advance Premium Tax Credit Payments
March 2017	
2017-43-022	Affordable Care Act: Verification of Premium Tax Credit Claims During the 2016 Filing Season (Funds Put to Better Use: $128,661,513; Taxpayer Rights and Entitlements: $6,668,090 impacting 15,118 taxpayer accounts; Taxpayer Burden: 13,381 taxpayer accounts impacted)
2017-10-019	Resolution of Defense Contract Audit Agency Findings of Questioned Contractor Costs Need Significant Improvement (Reliability of Information: $30,890,692)
2017-10-018	Status of Digital Accountability and Transparency Act Implementation Efforts
2017-10-020	Continuity Planning and Emergency Preparedness Follow-Up Audit
2017-40-026	Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers (Taxpayer Rights and Entitlements: 2,028,042 taxpayer accounts impacted; Taxpayer Burden: 2,754,104 taxpayer accounts impacted)
2017-10-023	Some Managerial Salaries Were Calculated Incorrectly Due to Complex Pay-Setting Rules (Inefficient Use of Resources: $3,626,274 impacting 630 employee accounts)
2017-30-025	Criminal Investigation Enforced Structuring Laws Primarily Against Legal Source Funds and Compromised the Rights of Some Individuals and Businesses (Taxpayer Burden: $17,100,000; Taxpayer Rights and Entitlements: 20 taxpayer accounts impacted)
2017-40-028	Interim Results of the 2017 Filing Season

Appendix III

TIGTA's Statutory Reporting Requirements

TIGTA issued one audit report required by statute dealing with the adequacy and security of IRS technology during this reporting period. In FY 2017, TIGTA will complete its 16th round of statutory reviews that are required annually by RRA 98. It will also complete its annual review of the Federal Financial Management Improvement Act (FFMIA) of 1996, the Office of National Drug Control Policy (ONDCP) Detailed Accounting Submission and Assertions, the Government Charge Card Abuse Prevention Act of 2012, Executive Order 13520 – Reducing Improper Payments and Eliminating Waste in Federal Programs, and the Improper Payments Elimination and Recovery Act of 2010 (IPERA). The following table reflects the FY 2017 statutory reviews.

Reference to Statutory Coverage	Explanation of the Provision	Comments/TIGTA Audit Status
Enforcement Statistics Internal Revenue Code (I.R.C.) Section (§) 7803(d)(1)(A)(i)	Requires TIGTA to evaluate the IRS's compliance with restrictions under RRA 98 § 1204 on the use of enforcement statistics to evaluate IRS employees.	Fieldwork currently in progress.
Restrictions on Directly Contacting Taxpayers I.R.C. § 7803(d)(1)(A)(ii)	Requires TIGTA to evaluate the IRS's compliance with restrictions under I.R.C. § 7521 on directly contacting taxpayers who have indicated they prefer their representatives be contacted.	Fieldwork currently in progress.
Filing of a Notice of Lien I.R.C. § 7803(d)(1)(A)(iii)	Requires TIGTA to evaluate the IRS's compliance with required procedures under I.R.C. § 6320 (a) upon the filing of a notice of lien.	Fieldwork currently in progress.
Extensions of the Statute of Limitations for Assessment of Tax I.R.C. § 7803(d)(1)(C) I.R.C. § 6501(c)(4)(B)	Requires TIGTA to include information regarding extensions of the statute of limitations for assessment of tax under I.R.C. § 6501 and the provision of notice to taxpayers regarding the right to refuse or limit the extension to particular issues or a particular period of time.	Fieldwork currently in progress.
Levies I.R.C. § 7803(d)(1)(A)(iv)	Requires TIGTA to evaluate the IRS's compliance with required procedures under I.R.C. § 6330 regarding levies.	Fieldwork currently in progress.
Collection Due Process I.R.C. § 7803(d)(1)(A)(iii) and (iv)	Requires TIGTA to evaluate the IRS's compliance with required procedures under I.R.C. §§ 6320 and 6330 regarding taxpayers' rights to appeal lien or levy actions.	Fieldwork currently in progress.

Reference to Statutory Coverage	Explanation of the Provision	Comments/TIGTA Audit Status
Seizures I.R.C. § 7803(d)(1)(A)(iv)	Requires TIGTA to evaluate the IRS's compliance with required procedures under I.R.C. §§ 6330 through 6344 when conducting seizures.	Fieldwork currently in progress.
Taxpayer Designations – Illegal Tax Protester Designation and Similar Designations I.R.C. § 7803(d)(1)(A)(v)	An evaluation of the IRS's compliance with restrictions under RRA 98 § 3707 on the designation of taxpayers.	Fieldwork currently in progress.
Disclosure of Collection Activities With Respect to Joint Returns I.R.C. § 7803(d)(1)(B) (TIGTA requirement) I.R.C. § 6103(e)(8) (IRS requirement)	Requires TIGTA to review and certify whether the IRS is complying with I.R.C. § 6103(e) (8) to disclose information to an individual filing a joint return on collection activity involving the other individual filing the return.	Fieldwork currently in progress.
Taxpayer Complaints I.R.C. § 7803(d)(2)(A)	Requires TIGTA to include in each of its Semiannual Reports to Congress the number of taxpayer complaints received and the number of employee misconduct and taxpayer abuse allegations received by IRS or TIGTA from taxpayers, IRS employees, and other sources.	Statistical results on the number of taxpayer complaints received are shown on page 67.
Administrative or Civil Actions With Respect to the Tax Collection Practices Act of 1996 I.R.C. § 7803(d)(1)(G) I.R.C. § 6304 RRA 98 § 3466	Requires TIGTA to include information regarding any administrative or civil actions with respect to violations of the fair debt collection provision of I.R.C. § 6304, including a summary of such actions and any resulting judgments or awards granted.	Fieldwork currently in progress.
Denial of Requests for Information I.R.C. § 7803(d)(1)(F) I.R.C. § 7803(d)(3)(A)	Requires TIGTA to include information regarding improper denial of requests for information from the IRS, based on a statistically valid sample of the total number of determinations made by the IRS to deny written requests to disclose information to taxpayers on the basis of I.R.C. § 6103 or 5 U.S.C. § 552(b)(7).	Fieldwork currently in progress.
Adequacy and Security of the Technology of the IRS I.R.C. § 7803(d)(1)(D)	Requires TIGTA to evaluate the IRS's adequacy and security of its technology.	Security Reviews: Ref. No. 2017-20-004, October 2017
Federal Financial Management Improvement Act of 1996 (FFMIA) 31 U.S.C. § 3512	Requires TIGTA to evaluate the financial management systems to ensure compliance with Federal requirements or the establishment of a remediation plan with resources, remedies, and intermediate target dates to bring the IRS into substantial compliance.	Fieldwork currently in progress.

Reference to Statutory Coverage	Explanation of the Provision	Comments/TIGTA Audit Status
Office of National Drug Control Policy (ONDCP) Detailed Accounting Submission and Assertions National Drug Enforcement Policy 21 U.S.C. § 1704(d) and the Office of National Drug Control Policy Circular entitled Drug Control Accounting, dated May 1, 2007.	Requires TIGTA to authenticate the IRS's ONDCP detailed accounting submission and assertions.	Ref. No. 2017-10-016, January 2017 The IRS did not implement TIGTA's prior recommendation to update its performance goals for FY 2017 to reflect prior performance and its own documented methodology. Otherwise, based on TIGTA's review, nothing came to our attention that caused us to believe that the assertions in the Detailed Accounting Submission and Performance Summary Report are not fairly presented in all material respects in accordance with the ONDCP's established criteria.
Government Charge Card Abuse Prevention Act of 2012 Pub. L. No. 112-194, 126 Stat. 1445.	Requires TIGTA to report on IRS progress in implementing purchase and travel card audit recommendations.	Ref. No. 2017-10-015, January 2017 The IRS properly identified and reported 21 instances of confirmed purchase card misuse and four instances of potential purchase card misuse pending final agency action. The 21 confirmed purchase card misuse cases reported by the IRS collectively totaled about $1,250. Additionally, TIGTA reviewed the status of the recommendations related to IRS purchase and travel cards issued over the past five fiscal years (FYs 2012 to 2016) and did not find any open recommendations.
Improper Payments Elimination and Recovery Act of 2010 (IPERA) 31 U.S.C. § 3321	Requires TIGTA to assess the IRS's compliance with improper payment requirements.	Fieldwork currently in progress.
Digital Accountability and Transparency Act of 2014 (DATA Act) Pub. L. No. 113-101, 128 Stat. 1124	Requires TIGTA to assess the completeness, timeliness, quality and accuracy of data that the IRS submits to comply with the DATA Act.	2017-10-018, March 2017 The IRS has made progress in its efforts to implement the requirements of the DATA Act, but much work remains. TIGTA identified areas that require additional attention. Specifically, the IRS did not clearly identify the source for 18 of the 57 data elements or document how the 57 data elements are used in its business processes as required. In addition, the IRS has not finalized the accounting procedures needed to support the posting of transaction-level grant program information in its financial system as required by the DATA Act.

Appendix IV

Section 1203 Standards

In general, the Commissioner of Internal Revenue shall terminate any IRS employee if there is a final administrative or judicial determination that, in the performance of official duties, such employee committed any misconduct violations outlined below. Such termination shall be a removal for cause on charges of misconduct.

Misconduct violations include:

- Willfully failing to obtain the required approval signatures on documents authorizing the seizure of a taxpayer's home, personal belongings, or business assets;
- Providing a false statement under oath with respect to a material matter involving a taxpayer or taxpayer representative;
- Violating, with respect to a taxpayer, taxpayer representative, or other employee of the IRS, any right under the Constitution of the United States, or any civil right established under Title VI or VII of the Civil Rights Act of 1964; Title IX of the Education Amendments of 1972; Age Discrimination in Employment Act of 1967; Age Discrimination Act of 1975; Section 501 or 504 of the Rehabilitation Act of 1973; or Title I of the Americans With Disabilities Act of 1990;
- Falsifying or destroying documents to conceal mistakes made by any employee with respect to a matter involving a taxpayer or taxpayer representative;
- Committing assault or battery on a taxpayer, taxpayer representative, or another employee of the IRS, but only if there is a criminal conviction or a final judgment by a court in a civil case with respect to the assault or battery;
- Violating the Internal Revenue Code of 1986, as amended (the Code), the Department of the Treasury regulations, or policies of the IRS (including the Internal Revenue Manual) for the purpose of retaliating against or harassing a taxpayer, taxpayer representative, or other employee of the IRS;
- Willfully misusing provisions of § 6103 of the Code for the purpose of concealing information from a congressional inquiry;
- Willfully failing to file any return of tax required under the Code on or before the date prescribed therefore (including any extensions), unless such failure is due to reasonable cause and not to willful neglect;
- Willfully understating Federal tax liability, unless such understatement is due to reasonable cause and not to willful neglect; and

- Threatening to audit a taxpayer for the purpose of extracting personal gain or benefit.

The Commissioner of Internal Revenue may mitigate the penalty of removal for the misconduct violations outlined above. The exercise of this authority shall be at the sole discretion of the Commissioner and may not be delegated to any other officer. The Commissioner, in his or her sole discretion, may establish a procedure that will be used to decide whether an individual should be referred to the Commissioner for determination. Any mitigation determination by the Commissioner in these matters may not be appealed in any administrative or judicial proceeding.

Appendix V

Implementing Section 989C of the Dodd-Frank Wall Street Reform and Consumer Protection Act

Inspector General Peer Review Activity
October 1, 2016 – March 31, 2017

No Peer Reviews Conducted of TIGTA's Office of Audit

No peer reviews were conducted of the TIGTA Office of Audit during this reporting period. In accordance with the three-year cycle, no external peer review was required during this reporting period.

No Peer Reviews Conducted by TIGTA's Office of Audit:

No peer reviews were conducted by the TIGTA Office of Audit during this reporting period

No Peer Reviews Conducted of TIGTA's Office of Investigations:

No peer reviews were conducted of the TIGTA Office of Investigations during this reporting period.

No Peer Reviews Conducted by TIGTA's Office of Investigations:

No peer reviews were conducted by the TIGTA Office of Investigations during this reporting period.

No Peer Reviews Conducted of TIGTA's Office of Inspections and Evaluations

No peer reviews were conducted of the TIGTA Office of Inspections and Evaluations during this reporting period.

No Peer Reviews Conducted by TIGTA's Office of Inspections and Evaluations

No peer reviews were conducted by the TIGTA Office of Inspections and Evaluations during this reporting period.

Appendix VI

Data Tables Provided by the Internal Revenue Service

The memorandum copied below is the IRS's transmittal to TIGTA. The tables that follow the memorandum contain information that the IRS provided to TIGTA and consist of IRS employee misconduct reports from the IRS Automated Labor and Employee Relations Tracking System (ALERTS) for the period October 1, 2016 through March 31, 2017. Also, data concerning substantiated RRA 98 §1203 allegations for the same period are included. IRS management conducted inquiries into the cases reflected in these tables.

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

HUMAN CAPITAL OFFICE

April 3, 2017

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

FROM: Constance L. Weaver
Acting Director, Workforce Relations Division

SUBJECT: Input for the Treasury Inspector General for Tax Administration (TIGTA) Semiannual Report to Congress

In response to your memorandum on January 26, 2017, I am providing the following information to meet your reporting requirements as defined in 26 U.S.C. §7803(d)(1)(E) and 26 U.S.C. §7803(d)(2)(A)(ii) for October 1, 2016, through March 31, 2017.

- Report of Employee Misconduct by Disposition Groups
- Report of Employee Misconduct – National Summary
- Summary of Substantiated Section 1203 Inquiries Recorded in Automated Labor and Employee Relations Tracking System (ALERTS)

The attached tables contain information about:

- Alleged misconduct reported to IRS managers
- Disposition of the allegations resolved during the period
- Status of the inventory as of March 31, 2016

The tables contain information about alleged misconduct that both TIGTA and IRS management investigated. The IRS received these allegations from taxpayers, IRS employees, and other sources, and recorded them in ALERTS.

The Summary of Substantiated Section 1203 Allegations contains information on the disposition of substantiated Section 1203 allegations. During this period, IRS managers substantiated 130 Section 1203 allegations and removed 13 employees as a result. Five (5) employees retired or resigned before a final administrative action by management and 3 employees were removed on other allegations. In two (2) of the removals, IRS management considered information in a TIGTA investigation. The Commissioner mitigated proposed removals in 14 cases. The remaining 95 substantiated allegations are still in the adjudication process.

Please note, some of the figures above do not match the Summary of Substantiated I.R.C. Section 1203 Inquiries Report figures. Protection of tax information is required when there are three or less cases, which are indicated by the asterisk in the report; however, the correct figures are included above.

If you have any questions, please contact Sheila Barbee, Acting Associate Director, LR/ER Field Operations at (202) 317-3307.

Attachments (3)

cc: John A. Koskinen, Commissioner of Internal Revenue
Kirsten Wielobob, Deputy Commissioner for Services and Enforcement
Jeffrey Tribiano, Deputy Commissioner for Operations Support
Nina Olson, National Taxpayer Advocate
Elita Christiansen, Executive Director, Equity, Diversity and Inclusion
Terry Lemons, Chief, Communications & Liaison
Mark Kaizen, Associate Chief Counsel (GLS)
Daniel T. Riordan, Chief Human Capital Officer

The Following Tables Are Provided by the IRS.

Report of Employee Misconduct by Disposition Groups

Period Covering October 1, 2016 - March 31, 2017

Disposition	TIGTA Report of Investigation	Administrative Case	Employee Tax Compliance Case	Employee Character Investigation	Totals
REMOVAL (PROBATION PERIOD COMPLETE)	18	43	13	1	**75**
REMOVAL AT OPM DIRECTION	0	0	0	7	**7**
PROBATION/SEPARATION	4	145	1	5	**155**
SEPARATION OF TEMP	0	1	0	0	**1**
RESIGN.,RET., ETC. (SF50 NOTED)	9	16	10	1	**36**
RESIGN. RET., ETC. (SF50 NOT NOTED)	19	102	29	1	**151**
SUSP., 14 DAYS OR LESS	46	92	76	0	**214**
SUSP., MORE THAN 14 DAYS	16	20	22	0	**58**
INDEFINITE SUSPENSION	0	5	0	0	**5**
REPRIMAND	42	133	121	3	**299**
ADMONISHMENT	34	183	305	0	**522**
WRITTEN COUNSELING	45	188	193	4	**430**
ORAL COUNSELING	0	30	16	0	**46**
A D: IN LIEU OF REPRIMAND	6	13	9	0	**28**
A D: IN LIEU OF SUSPENSION	7	13	20	0	**40**
CLEARANCE LETTER	57	84	4	0	**145**
CWA CAUTIONARY LTR	86	183	122	42	**433**
CWA LETTER	68	109	40	3	**220**
TERMINATION FOR ABONDOMENT OF POSITION	0	0	0	0	**23**
PROSECUTION PENDING FOR TIGTA'S ROI	1	0	0	0	**1**
FORWARDED TO TIGTA	0	2	0	0	**2**
TOTAL	**458**	**1385**	**981**	**67**	**2891**

Source: Automated Labor and Employee Relations Tracking System (ALERTS)

This report is being produced in accordance with 26 USC §7803(d)(2) and §4(a)2 of Treasury Delegation Order 115-01, January 14, 1999

Note: AD is abbreviation for Alternative Discipline

Extract Date: April 4, 2017

Report of Employee Misconduct National Summary

Period Covering October 1, 2016 - March 31, 2017

Inventory Case Type	Open Inventory	Conduct Cases Received	Cases Closed			Ending Inventory
			Conduct Issues	Cases Merged with Other Cases	Non-Conduct Issues	
ADMINISTRATIVE CASE	649	1857	1709	68	63	666
EMPLOYEE CHARACTER INVESTIGATION	29	92	70	1	0	50
EMPLOYEE TAX COMPLIANCE CASE	936	1227	1029	32	0	1102
TIGTA REPORT OF INVESTIGATION	589	603	555	11	0	626
Total	2203	3779	3363	112	63	2444

Source: Automated Labor and Employee Relations Tracking System (ALERTS)

TIGTA Investigations (ROI) - Any matter involving an employee in which TIGTA conducted an investigation into alleged misconduct and referred a Report of Investigation (ROI) to IRS for appropriate action.

Administrative Case - Any matter involving an employee in which management conducted an inquiry into alleged misconduct.

Employee Tax Compliance Case - Any conduct matter that is identified by the Employee Tax Compliance program which becomes a matter of official interest.

Background Investigations - Any matter involving a New Background Investigation Case (NBIC) investigation into an employee's background that is referred to management for appropriate action.

Extract Date: April 3, 2017

Summary of Substantiated I.R.C. Section 1203 Inquiries Recorded in ALERTS

Period Covering October 1, 2016 - March 31, 2017

§ 1203 Violation	*Removals	*Resigned/ Retired	Probation Separation	Removed On Other Grounds	*Penalty Mitigated	In Personnel Process	Total
1203(b)(10): THREAT OF AUD/PERSONAL	0	0	0	0	0	2	2
1203(b)(4): CONCEALED WORK ERROR	0	0	0	0	0	3	3
1203(b)(6): IRC/IRM/REG VIOL-RETAL	0	0	0	1	0	1	2
1203(b)(8): WILLFUL UNTIMELY RETURN	8	0*	0	0	9	46	65
1203(b)(9): WILLFUL UNDERSTATED TAX	5	3	0	0*	5	43	58
Total	13	5	0	3	14	95	130

Source: Automated Labor and Employee Relations Tracking System (ALERTS).

Note: The cases reported as "Removals" and" Penalty Mitigated" do not reflect the results of any third party appeal.

Columns containing numbers of two or less and protected by I.R.C. Section 6103 are annotated with a zero.

*These cases are included in the totals of the Table entitled "Reports of Employee Misconduct Summary by Disposition Groups"

This report is being produced in accordance with 26 USC §7803(b)(2) and §4(a)(2) of Treasury Delegation Order 115-01, January 14, 1999

Extract Date: April 3, 2017

Glossary of Acronyms

ACTC	Additional Child Tax Credit
AOTC	American Opportunity Tax Credit
CI	IRS Criminal Investigation
CTC	Child Tax Credit
EEFax	Enterprise e-fax
FCC	Federal Communications Commission
FTC	Federal Trade Commission
FY	Fiscal Year
GPR	General Purpose Reloadable
HCTC	Health Care Tax Credit
HROA	HR Outsourcing Associates, Inc.
HUD	U.S. Department of Housing and Urban Development
I&E	Office of Inspections and Evaluations
I.R.C.	Internal Revenue Code
IP PIN	Identity Protection Personal Identification Number
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
OEP	Office of Employee Protection
OI	Office of Investigations
PATH Act	Protecting Americans from Tax Hikes Act of 2015
PII	Personally identifiable information
PIN	Personal Identification Number
PTIN	Preparer Tax Identification Number
PY	Processing Year
RRA 98	Internal Revenue Service Restructuring and Reform Act of 1998
RTR	Remittance Transaction Research
SB/SE	Small Business/Self-Employed Division (IRS)
TAC	Taxpayer Assistance Center
TFRP	Trust Fund Recovery Penalty
TIGTA	The Treasury Inspector General for Tax Administration
TY	Tax Year
U.S.C.	United States Code
USCIS	U.S. Citizen and Immigration Services

ACRONYMS USED EXCLUSIVELY IN APPENDICES	
ACS	Automated Collection System
AIMS	Audit Information Management System
ALERTS	Automated Labor and Employee Relations Tracking System
ARDI	Accounts Receivable Dollar Inventory
CO	Contracting Officer
DATA	Digital Accountability and Transparency Act of 2014
DCAA	Defense Contract Audit Agency
ECC	Enterprise Computing Center
FFMIA	Federal Financial Management Improvement Act
FIPS	Federal Information Processing Standard
FIT	Final Integration Test
IBC	International Business Compliance
ICS	Integrated Collection System
IDRS	Integrated Data Retrieval System
IPERA	Improper Payments Elimination and Recovery Act
KISAM-AM	Knowledge, Incident/Problem, Service Asset Management Asset Manager
LB&I	Large Business and International
LUQ	Large, Unusual, or Questionable
NFTL	Notice of Federal Tax Lien
ONDCP	Office of National Drug Control Policy
PCLIA	Privacy and Civil Liberties Impact Assessment
SA&A	Security Assessment and Authorization
SBU	Sensitive But Unclassified
SME	Subject Matter Expert
SRS	Specialist Referral System
SSA	Social Security Administration
TAS	Taxpayer Advocate Service
TASIS	Taxpayer Advocate Service Integrated System
TIC	Trusted Internet Connection
TPP	Transfer Pricing Practice

Call our toll-free hotline to report waste, fraud, or abuse:

1-800-366-4484

By Web:

www.tigta.gov

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, DC 20044-0589

Information you provide is confidential and you may remain anonymous

Department of the Treasury

Office of the Inspector General for Tax Administration
1401 H Street, NW., Suite 469
Washington, DC 20005

This report and complete copies of TIGTA audit reports are available online at: www.tigta.gov