HEARING BEFORE THE
COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

"Protection of Taxpayers' Personal Information"

Testimony of
The Honorable J. Russell George
Treasury Inspector General for Tax Administration

April 14, 2016

Washington, D.C.

TESTIMONY
OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

"Protection of Taxpayers' Personal Information"
April 14, 2016

Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittee, thank you for the opportunity to testify on the Internal Revenue Service's (IRS) process to prevent unauthorized access to taxpayer data.

The Treasury Inspector General for Tax Administration (TIGTA) is statutorily mandated to provide independent audit and investigative services necessary to improve the economy, efficiency, and effectiveness of IRS operations, including the IRS Chief Counsel. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA's role is critical in that we provide the American taxpayer with assurance that the approximately 86,000 IRS employees[1] who collected over $3.3 trillion in tax revenue, processed over 244 million tax returns, and issued more than $400 billion in tax refunds during Fiscal Year (FY) 2015,[2] have done so in an effective and efficient manner while minimizing the risks of waste, fraud, and abuse.

TIGTA's Office of Audit (OA) reviews all aspects of the Federal tax administration system and provides recommendations to: improve IRS systems and operations; ensure the fair and equitable treatment of taxpayers; and detect and prevent waste, fraud, and abuse in tax administration. The Office of Audit has examined specific high-risk issues such as identity theft, refund fraud, improper payments, information technology, security vulnerabilities, complex modernized computer systems, tax collections and revenue, and waste and abuse in IRS operations.

TIGTA's Office of Investigations (OI) protects the integrity of the IRS by investigating allegations of IRS employee misconduct, external threats to IRS

---

[1] Total IRS staffing as of October 3, 2015. Included in the total are approximately 15,400 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2015*.

employees and facilities, and other attempts to impede or otherwise interfere with the IRS's ability to collect taxes. Specifically, the Office of Investigations investigates misconduct by IRS employees which manifests itself in many ways, including unauthorized access to taxpayer information and the use of the information for the purposes of identity theft; extortion; theft of government property; taxpayer abuses; false statements; and other financial fraud. The Office of Investigations is statutorily charged to investigate threats made against the IRS's employees, facilities and data. We are committed to ensuring the safety of IRS employees and the taxpayers who conduct business at the approximately 550 offices[3] in the United States and abroad.

TIGTA's Office of Inspections and Evaluations performs responsive, timely, and cost-effective inspections and evaluations of challenging areas within the IRS, providing TIGTA with additional flexibility and capability to produce value-added products and services to improve tax administration. Inspections are intended to monitor compliance with applicable laws, regulations, and/or policies; assess the effectiveness and efficiency of programs and operations; and inquire into allegations of waste, fraud, abuse, and mismanagement. Evaluations, on the other hand, are intended to provide in-depth reviews of specific management issues, policies, or programs.

Cybersecurity threats against the Federal Government continue to grow. Since 2011, my office has identified the security of taxpayer data as the most serious management and performance challenge confronting the IRS. According to the Department of Homeland Security's U.S. Computer Emergency Readiness Team, Federal agencies reported 77,183 cyberattacks in FY 2015, an increase of more than 10 percent from FY 2014.[4]

The IRS, the largest component of the Department of the Treasury, has primary responsibility for administering the Federal tax system. The IRS's role is unique within the Federal Government in that it administers the Nation's tax laws and collects the revenue that funds the Government. It also works to protect Federal revenue by detecting and preventing the growing risk of fraudulent tax refunds and other improper payments. The IRS relies extensively on its computer systems to support both its financial and mission-related operations. These computer systems collect and process extensive amounts of taxpayer data, including Personally Identifiable Information. For Calendar Year 2015, the IRS processed more than 150 million individual tax returns and

---

[3] IRS, *Management's Discussion & Analysis, Fiscal Year 2015*.
[4] Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act* (Mar. 2016).

more than 55 million business tax returns that contain taxpayers' sensitive financial data.

TIGTA has identified a number of areas in which the IRS could better protect taxpayer data and improve its overall security position. My comments today will focus on our work related to the IRS's processes to authenticate users accessing its online services and the IRS's ability to prevent and detect breaches to its computer systems.

IRS AUTHENTICATION PROCESSES NEED IMPROVEMENT

The increasing number of data breaches in the private and public sectors means more personal information than ever before is available to unscrupulous individuals. Much of these data are detailed enough to enable circumvention of most authentication processes. Therefore, it is critical that the methods 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.

The risk of unauthorized access to tax accounts will continue to grow as the IRS focuses its efforts on delivering online tools to taxpayers. The IRS's goal is to eventually provide taxpayers with dynamic online account access that includes viewing their recent payments, making minor changes and adjustments to their accounts, and corresponding digitally with the IRS.

The IRS recognized that there was a lack of consistency in the techniques it had employed for authentication; therefore, in June 2014, it established the Authentication Group. In a report issued in November 2015, TIGTA found that although the IRS recognizes the growing challenge it faces in establishing effective authentication processes and procedures, the IRS has not established a Service-wide approach to managing its authentication needs.[5] As a result, the level of authentication the IRS uses for its various services is not consistent. Specifically, TIGTA found that while the Authentication Group is evaluating potential improvements to existing authentication methods for the purpose of preventing identity theft, it is not developing overall strategies to enhance authentication methods across IRS functions and programs. TIGTA recommended that the IRS develop a Service-wide strategy that establishes consistent oversight of all authentication needs across IRS functions and programs. In addition, the IRS should ensure that responsibility for implementing the strategy is optimally aligned to provide centralized oversight and facilitate decision making for the

---

[5] TIGTA, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).

development and integration of all forms of authentication, including frameworks, policies, and processes across the IRS.

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. Unscrupulous individuals can identify the weakest points of authentication and exploit them to inappropriately gain access to tax account information. For example, on May 26, 2015, the IRS announced that unauthorized access attempts were made by individuals using taxpayer-specific data to gain access to tax information[6] through its Get Transcript application. According to the IRS, one or more individuals succeeded in clearing the IRS's authentication process that required knowledge of information about the taxpayer, including Social Security information, date of birth, tax filing status, and street address. To prevent further unauthorized accesses, the IRS removed the application from its website.

Office of Management and Budget (OMB) Memorandum M-04-04, *E-Authentication for Federal Agencies,*[7] establishes criteria for determining the risk-based level of authentication assurance required for specific electronic applications and transactions. E-Authentication is the process of establishing confidence in user identities electronically presented to an information system. The OMB guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. This guidance is intended to help agencies identify and analyze the risks associated with each step of the authentication process. As the outcome of an authentication error becomes more serious, the required level of assurance increases.

In addition, the U.S. Department of Commerce National Institute of Standards and Technology (NIST) *Special Publication 800-63-2, Electronic Authentication Guideline*[8] provides the technical requirements for the four levels of assurance defined in OMB guidance as shown in the following table.

---

[6] The tax information that can be accessed on the Get Transcript application can include the current and three prior years of tax returns, nine years of tax account information, and wage and income information.
[7] OMB, M-04-04, *E-Authentication for Federal Agencies* (Dec. 2003).
[8] NIST, NIST SP-800-63-2, *Electronic Authentication Guideline* (Aug. 2013).

Table 1 - Levels of Electronic Assurance

Level of Assurance	Requirements	Level of Confidence
Level 1	No identity proofing is required.	Provides little or no confidence.
Level 2	Requires basic identity proofing data, a valid current Government identification number, and a valid financial or utility account number. Access occurs only after identity proofing data and either the Government identification number or financial/utility account number are verified by the agency.	Provides some confidence in the validity of an individual's identity.
Level 3	Requires basic identity proofing data, a valid current Government identification number, and a valid financial or utility account number as well as the use of a second authentication factor such as a one-time supplemental code issued via text message or e-mail to the telephone number or e-mail address associated with the individual.	Provides high confidence in the validity of an individual's identity.
Level 4	Requires in-person identity proofing and verification.	Provides very high confidence in the validity of an individual's identity.

OMB standards require Federal agencies to conduct an assessment of the risk of authentication error for each online service or application they provide. An authentication error occurs when an agency confirms the identity provided by an individual when in fact the individual is not who he or she claims to be. In addition, NIST Special Publication 800-63 establishes specific requirements that agencies' authentication processes must meet to provide a specific level of authentication assurance. However, we found that, although the IRS has established processes and procedures to authenticate individuals requesting online access to IRS services, these processes and procedures do not comply with Government standards for assessing authentication risk and establishing adequate authentication processes.

Our analysis of the e-Authentication processes used to authenticate users of the IRS's online Get Transcript and Identity Protection Personal Identification Number (IP PIN)[9] applications found that these authentication methods provide only single-factor authentication despite NIST standards requiring multifactor authentication for such high-risk applications.

[9] To provide relief to tax-related identity theft victims, the IRS issues IP PINs to taxpayers who are confirmed by the IRS as victims of identity theft, taxpayers who are at a high risk of becoming a victim such as taxpayers who call reporting a lost or stolen wallet or purse, as well as taxpayers who live in three locations that the IRS has identified as having a high rate of identity theft (Florida, Georgia and the District of Columbia).

In addition, the IRS's current e-Authentication framework does not comply with NIST standards for single-factor authentication. Specifically, the e-Authentication framework does not require individuals to provide Government identification or a financial or utility account number, as required by NIST standards. According to IRS management, the IRS decided to not request financial or utility account information because the information cannot currently be verified. IRS management informed us that the IRS obtained and verified the taxpayer filing status to mitigate the risk of its being unable to use financial information to authenticate individuals.

Although the IRS required taxpayers to provide a filing status, this requirement does not bring it into compliance with NIST standards, and the IRS remains noncompliant with single-factor authentication requirements. The IRS received guidance from the NIST at the time the e-Authentication framework was being developed indicating that a Taxpayer Identification Number (TIN) was an acceptable form of identification. However, in August 2015, the NIST informed us that a TIN is not currently an acceptable Government identification number for the purpose of authentication. We brought this discrepancy to the IRS's attention and IRS management agreed that a TIN is no longer an acceptable form of identification. Management also indicated that the IRS would take steps to conform to NIST standards for verifying an individual's identity.

The IRS assessed the risk of the Get Transcript application as required. However, the IRS determined that the authentication risk associated with Get Transcript was low to both the IRS and taxpayers. The IRS defines a low risk rating as one in which the likelihood of an imposter obtaining and using the information available on an application is low. In addition, a low risk rating indicates that controls are in place to prevent, or at least significantly impede, an imposter from accessing the information. As a result, the IRS implemented single-factor authentication to access the Get Transcript application.

In August 2015, the IRS indicated that unauthorized users had been successful[10] in obtaining information on the Get Transcript application for an estimated 334,000 taxpayer accounts. TIGTA's current review[11] of the Get Transcript breach identified additional suspicious accesses to taxpayers' accounts that the IRS had not identified. Based on TIGTA's analysis of Get Transcript access logs, the IRS

---

[10] A successful access is one in which the unauthorized users successfully answered identity proofing and knowledge-based authentication questions required to gain access to taxpayer account information.
[11] TIGTA, Audit No. 201540027, *Evaluation of Assistance Provided to Victims of the Get Transcript Data Breach*, report planned for May 2016.

reported on February 26, 2016 that potentially unauthorized users had been successful in obtaining access to an additional 390,000 taxpayer accounts. The IRS also reported that an additional 295,000 taxpayer transcripts had been targeted but the access attempts had not been successful. TIGTA was able to identify the additional unauthorized accesses due to our use of advanced analytics and cross-discipline approaches. The IRS had not previously identified these accesses because of limitations in the scope of its analysis, including its method of identifying suspicious e-mail accounts and the time frame it analyzed.

In response to TIGTA's identification of the additional accesses, the IRS started on February 29, 2016 mailing notification letters to the affected taxpayers and placing identity theft markers on their tax accounts. It should be noted that the actual number of individuals whose personal information was available to the potentially unauthorized individuals accessing these tax accounts is significantly greater than the number of taxpayers whose accounts were accessed because the tax accounts accessed include certain information on other individuals listed on a tax return (*e.g.*, spouses and dependents).

We are currently evaluating the appropriateness of the IRS's response to the Get Transcript incident and the IRS's proposed solutions to address the authentication weakness that allowed the incident to occur.[12] During our audit work, we have learned that the IRS is working with the U.S. Digital Service[13] on its new e-authentication and authorization policies and procedures. In addition, TIGTA is participating in a multi-agency investigation into this matter, and we have provided the IRS with some of our investigative observations to date in order to help them secure the e-authentication environment in the future.

We also reported in November 2015 that the IRS did not complete the required authentication risk assessment for its IP PIN application. In addition, on January 8, 2016, we recommended that the IRS not reactivate its online IP PIN application for the 2016 Filing Season, due to concerns that the IP PIN authentication process requires knowledge of the same taxpayer information that was used by unscrupulous individuals to breach the Get Transcript application. However, the IRS reactivated the application on January 19, 2016. We issued a second recommendation to the IRS on February 24, 2016, advising it to remove the IP PIN application from its public website.

---

[12] TIGTA, Audit No. 201520006, *Review of Progress to Improve Electronic Authentication*, report planned for July 2016.

[13] The U.S. Digital Service is part of the Executive Office of the President. Its goal is to improve and simplify the digital services that people and businesses have with the Government.

On March 7, 2016, the IRS reported that it was temporarily suspending use of the IP PIN application as part of an ongoing security review. The IRS reported that it is conducting a further review of the application that allows taxpayers to retrieve their IP PINs online and is looking at further strengthening its security features. The IRS does not anticipate having the technology in place for either the Get Transcript or IP PIN application to provide multifactor authentication capability before the summer of 2016.

No single authentication method or process will prevent unscrupulous individuals from filing identity theft tax returns or attempting to inappropriately access IRS services. However, strong authentication processes can reduce the risk of such activity by making it harder and more costly for such individuals to gain access to resources and information. Therefore, it is important that the IRS ensure that its authentication processes are in compliance with NIST standards in order to provide the highest degree of assurance required and to ensure that authentication processes used to verify individuals' identities are consistent among all methods used to access tax account information.

DATA SECURITY REMAINS A TOP CONCERN OF TIGTA

As previously mentioned in my testimony, TIGTA has designated the security of taxpayer data as the top concern facing the IRS based on the increased number and sophistication of threats to taxpayer information and the need for the IRS to better protect taxpayer data and improve its enterprise security program. TIGTA continues to identify significant security weaknesses that could affect the confidentiality, integrity, and availability of financial and sensitive taxpayer data. We have identified a number of areas in which the IRS could better protect taxpayer data and improve its overall security posture.

During our most recent Federal Information Security Modernization Act[14] evaluation of the IRS's information security programs and practices,[15] we found three security program areas, *i.e.,* Continuous Monitoring Management, Identity and Access Management, and Configuration Management, that did not meet the level of

---

[14] Pub. L. No. 113-283, 128 Stat. 3073 (2014). This bill amended chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.
[15] TIGTA, Ref. No. 2015-20-092, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2015* (Sept. 2015).

performance specified by the Department of Homeland Security.[16]

One of the Federal Government's latest security initiatives is the implementation of continuous monitoring of information security, which is defined as maintaining ongoing, real-time awareness of information security, vulnerabilities, and threats to support organizational risk decisions. While the IRS has made progress and is in compliance with guidelines from the Department of Homeland Security and the Department of the Treasury, we found that the IRS is still in the process of implementing its Information Security Continuous Monitoring program required by the Office of Management and Budget to automate asset management and maintain the secure configuration of assets in real time.

The Identity and Access Management program ensures that only those with a business need are able to obtain access to IRS systems and data. However, we found that this program did not meet a majority of the attributes specified by the Department of Homeland Security, largely due to the IRS's failure to achieve Government-wide goals set for implementing logical (system) and physical access to facilities in compliance with Homeland Security Presidential Directive 12 requirements. Homeland Security Presidential Directive 12 requires Federal agencies to issue personal identity verification cards to employees and contractors for accessing agency systems and facilities.

Configuration Management ensures that settings on IRS systems are maintained in an organized, secure, and approved manner that includes the timely installation of patches to resolve known security vulnerabilities. We found that the IRS has not fully implemented enterprise-wide automated processes to identify computer assets, evaluate compliance with configuration policies, and deploy security patches.

We have also identified other areas that would improve the IRS's ability to defend its systems against cyberattacks. Monitoring IRS networks 24 hours a day, year-round, for cyberattacks and responding to various computer security incidents is the responsibility of the IRS's Computer Security Incident Response Center (CSIRC). TIGTA evaluated the effectiveness of the CSIRC at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data, and

---

[16] To assist the Inspectors General in evaluating Federal agencies' compliance with the Federal Information Security Modernization Act, the Department of Homeland Security issued the *Fiscal Year 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, which specified 10 information security program areas and listed specific attributes within each area for evaluation.

identified areas for improvement.[17] At the time of our review, the CSIRC's host-based intrusion detection system was not monitoring a significant percentage of IRS servers, which leaves that portion of the IRS network and data at risk. In addition, the CSIRC was not reporting all computer security incidents to the Department of the Treasury, as required. Finally, incident response policies, plans, and procedures were nonexistent, inaccurate, or incomplete.

The IRS reported that more than 1,000 security incidents occurred to its systems during the period August 1, 2014, to July 31, 2015. We are currently evaluating the effectiveness of the CSIRC at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data, and plan to issue our report later this year.[18]

TIGTA also found that many interconnections[19] in use at the IRS do not have proper authorization or are not covered by security agreements. Although the IRS has established an office to provide oversight and guidance for the development of security agreements, that office is not responsible for managing or monitoring agreements for all external interconnections in use in the IRS environment. TIGTA believes the lack of a centralized inventory and of an enterprise-level approach to ensure that all external interconnections are monitored have contributed to interconnections that are active but lack proper approvals and assurances necessary to meet current security requirements.[20]

In addition, TIGTA reported[21] that the IRS was unable to upgrade all of its workstations with the most current Windows® operating system.[22] Because of their importance, operating systems must be updated on a regular basis to patch security vulnerabilities and, if necessary, upgraded completely in order to fix crucial weaknesses or to address new threats to their functionality. TIGTA found that the IRS did not follow established policies with respect to project management and provided inadequate

---

[17] TIGTA, Ref. No. 2012-20-019, *The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed* (Mar. 2012).
[18] TIGTA, Audit No. 201620003, *Effectiveness of the Computer Security Incident Response Center*, report planned for September 2016.
[19] The National Institute of Standards and Technology defines a system interconnection as the direct connection of two or more information technology systems for the purpose of sharing data and other information resources.
[20] TIGTA, Ref. No. 2015-20-087, *Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured* (Sept. 2015).
[21] TIGTA, Ref. No. 2015-20-073, *Inadequate Early Oversight Led to Windows Upgrade Project Delays* (Sept. 2015).
[22] The software that communicates with computer hardware to allocate memory, process tasks, access disks and peripherals, and serves as the user interface.

oversight and monitoring of the Windows upgrade early in its effort. As a result, the IRS had not accounted for the location or migration status of approximately 1,300 workstations and had upgraded only about one-half of its applicable servers at the conclusion of our audit.

We at TIGTA take seriously our mandate to provide independent oversight of the IRS in its administration of our Nation's tax system and will continue to expand our oversight related to cybersecurity. Based on the increased number and sophistication of threats to taxpayer information and the need for the IRS to better protect taxpayer data and improve its enterprise security program, we plan to provide continuing audit and investigative coverage of the IRS's efforts to protect the confidentiality of taxpayer information.

Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittee, thank you for the opportunity to share my views.