COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON OVERSIGHT
U.S. HOUSE OF REPRESENTATIVES

"The Internal Revenue Service's Taxpayer Online Authentication Efforts"

Testimony of
Michael E. McKenney
Deputy Inspector General for Audit
Treasury Inspector General for Tax Administration

September 26, 2018

Washington, D.C.

TESTIMONY
OF
MICHAEL E. McKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON OVERSIGHT

"The Internal Revenue Service's Taxpayer Online Authentication Efforts"
September 26, 2018

Chairman Jenkins, Ranking Member Lewis, and Members of the Subcommittee, thank you for the opportunity to discuss the Internal Revenue Service's (IRS) efforts to address electronic authentication on its online applications.

The Treasury Inspector General for Tax Administration (TIGTA) was created by Congress in 1998 with a statutory mandate of ensuring integrity in America's tax system. It provides independent audit and investigative services to improve the economy, efficiency, and effectiveness of IRS operations. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA plays the key role of ensuring that the approximately 79,000 IRS employees[1] who collected more than $3.4 trillion in tax revenue, processed more than 246 million tax returns, and issued more than $437 billion in tax refunds during Fiscal Year (FY) 2017,[2] have done so in an effective and efficient manner while minimizing the risk of waste, fraud, and abuse.

In my testimony, I will discuss the work that TIGTA has completed to address the IRS's ability to deploy secure electronic authentication on its online applications and to protect taxpayer data from unauthorized access.

INFORMATION SECURITY OVER TAXPAYER DATA

The IRS relies extensively on its computer systems to support both its financial and mission-related operations. These computer systems collect and process large amounts of taxpayer data. Recent cyber events against the IRS have illustrated that bad actors are continually seeking new ways to attack and exploit IRS computer

[1] Total IRS staffing as of September 1, 2018. Included in the total are approximately 16,650 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2017*.

systems and processes in order to access tax information for the purposes of identity theft and filing fraudulent claims for tax refunds. For example, in May 2015, the IRS discovered that criminals used taxpayers' personal identification information obtained from sources outside the IRS to impersonate the taxpayers and gain unauthorized access to tax information in its Get Transcript application. TIGTA believes that the system was widely exploited by numerous bad actors who collectively made at least 724,000 potentially unauthorized accesses to taxpayer accounts, resulting in the filing of 252,400 potentially fraudulent tax returns and the issuance of $490 million in potentially fraudulent refunds.

In March 2017, the IRS shut down its Data Retrieval Tool (DRT) on the Department of Education's Free Application for Federal Student Aid (FAFSA) web application when it discovered that identity thieves were using individuals' personal information that they obtained outside of the tax system to start the FAFSA application process in order to obtain Adjusted Gross Income tax information from the DRT. The IRS estimated that approximately 100,000 taxpayers were impacted by this data breach.

From the exploitation of IRS's Get Transcript application to that of the DRT, the IRS has found that, with each systemic weakness it closes, criminals have discovered another means to access tax information from the IRS. In addition, massive data breaches—such as those at Yahoo where up to 500 million customers may have had sensitive data stolen, at the U.S. Government Office of Personnel Management where 21.5 million current, former, and prospective Federal employees had their sensitive information, including Social Security Numbers, stolen, and at Equifax where 145 million Americans had their Social Security Numbers, dates of birth, addresses, and in some cases, driver's license numbers, exposed —illustrate the constant threat to protecting sensitive personal information and the increasing risk of identity theft. As the threat landscape continues to evolve, we believe that protecting the confidentiality of taxpayer information will continue to be a top concern for the IRS.

After the Get Transcript breach was discovered in May 2015, TIGTA assessed the IRS's efforts to authenticate taxpayer identities when services are provided to taxpayers. In our report, TIGTA made recommendations for the IRS to develop a Service-wide strategy that: establishes consistent oversight of all authentication needs across the IRS's functions and programs; ensures that the level of authentication risk for all current and future online applications accurately reflects the risk to the IRS and taxpayers should an authentication error occur; and ensures that the authentication

processes meet Government Information Security Standards.[3] The IRS agreed with these recommendations.

In December 2016, the IRS issued its Identity Assurance Strategy and Roadmap for developing a modern and secure authentication environment for all taxpayers, regardless of how they interact with IRS. This strategy and roadmap document contains six core authentication objectives as well as high-level strategic efforts and initiatives. Two specific initiatives are to integrate online applications behind a secure eAuthentication solution and to strengthen eAuthentication through enhanced identity proofing and expanded coverage, ensuring compliance with Federal regulations.

Following the Get Transcript breach, the IRS took positive steps in response to TIGTA's recommendations to provide more secure authentication, including the implementation of two-factor authentication and the strengthening of application and network controls.[4] However, TIGTA remains concerned about the IRS's logging and monitoring capabilities over all connections to IRS online services.

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. In February 2018, TIGTA reported that the IRS made progress in improving its electronic authentication controls.[5] For example, the IRS deployed a more rigorous electronic authentication process that provides two-factor authentication via a security code sent to text-enabled mobile phones. However, these improvements only applied to five online applications. The IRS also completed or updated electronic authentication risk assessments for 28 of its online applications to determine appropriate levels of authentication assurance, and enhanced its network monitoring and audit log analysis capabilities.

Our audit also identified that network monitoring tools that the IRS purchased to improve the prevention and detection of automated attacks were not fully implemented due to issues related to resources, incompatibility, and higher priorities. Controls to prevent fraudulent users from improperly creating profiles were not fully implemented. Further, the IRS is not fulfilling its requirements for monitoring audit logs for suspicious activity. This is due to inadequate processes for generating and reviewing audit log

---

[3] TIGTA, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).
[4] TIGTA, Ref. No. 2016-20-082, *Improvements Are Needed to Strengthen Electronic Authentication Process Controls* (Sept. 2016).
[5] TIGTA, Ref. No. 2018-20-007, *Electronic Authentication Process Controls Have Been Improved, But Have Not Yet Been Fully Implemented* (Feb. 2018).

reports as well as failure to ensure that reports are useful for investigating and responding to suspicious activities.

The risk of unauthorized access to tax accounts will continue to be significant as the IRS proceeds with expansion of the online tools it makes available to taxpayers.[6] The IRS's goal is to provide taxpayers with dynamic online tax account access that includes viewing their recent payments, making minor changes and adjustments to their tax accounts, and corresponding digitally with the IRS. In March 2018, TIGTA reported concerns over the IRS's Transcript Delivery System (TDS), which allows external third-party customers to view and obtain tax information of both individuals and businesses.[7] We found that processes and procedures to authenticate e-Services users, including those users accessing the TDS application, do not comply with Federal Government Information Security Standards. The IRS continued to use single-factor authentication to authenticate users even though a risk assessment in both Calendar Years 2011 and 2015 rated e-Services as requiring multifactor authentication.

TIGTA is currently evaluating whether the IRS has properly implemented secure electronic authentication controls in accordance with Federal standards for public access to IRS online systems. This audit is taking an enterprise view of how the IRS is addressing electronic authentication on all online systems. We anticipate issuing a final report in December 2018.

One of the challenges that the IRS faces is the recent issuance of new guidelines from the National Institute of Standards and Technology (also known as NIST). In June 2017, NIST issued Special Publication 800-63-3, *Digital Identity Guidelines*, which superseded Special Publication 800-63-2, *Electronic Authentication Guidelines*. NIST recognized the need to update its guidance to implement and manage digital identities because digital identity components have evolved substantially since it issued its Special Publication 800-63-2. The new guidelines replace the levels of assurance (no identity proofing required, basic identity proofing using single-factor authentication, more in-depth identity proofing using two-factor authentication, and in-person identity proofing

[6] Preparing the IRS to adapt to the changing needs of taxpayers is described generally as the IRS Future State initiative. A key part of this effort is for taxpayers to have a more complete online experience for their IRS interactions.
[7] TIGTA, Ref. No. 2018-40-014, *Transcript Delivery System Authentication and Authorization Processes Do Not Adequately Protect Against Unauthorized Release of Tax Information* (Mar. 2018).

and verification) with the components of digital identity services (identity proofing,[8] authentication management,[9] and federation and assertions[10]).

While we are still discussing the results of this current audit with the IRS, I can share some preliminary observations. The IRS has completed eAuthentication risk assessments for its 52 public-facing applications. Of these 52 applications, TIGTA found that the IRS secured 14 high-risk online applications and eight moderate-risk online applications and took four applications offline. As such, 26 online applications were not at their assessed level of eAuthentication levels of assurance. The IRS is accepting the risks associated with half of its public-facing applications not meeting the necessary level of assurance, and TIGTA found the IRS's rationale for maintaining them at the current level was reasonable based on the IRS transaction analysis and compensating controls to mitigate risks. These risk assessments were based on the old NIST guidelines. The IRS was in the middle of bringing the remaining applications to their appropriate authentication levels when new NIST guidelines were issued.

During the past year, the IRS has been transitioning to the new NIST guidelines. A new process called the Digital Identity Risk Assessment process was created to redesign the old eAuthentication risk assessments. In addition, the IRS established supporting processes, such as completing an assessment tool to collect various parameters of online transactions and to calculate levels of assurances, and it also began providing monthly updates to IRS executives.

In July 2018, the IRS piloted this new process on one of its applications and is moving forward with applying this process to its other online applications. Because the IRS has not completed its risk assessments based on the new NIST guidelines, the IRS cannot say whether its 52 online applications are at their appropriate levels of authentication assurance.

To identify abnormalities in accesses to the IRS eAuthentication application, the IRS established the Cybersecurity Fraud Analytics and Monitoring (CFAM) group after the eAuthentication breach in May 2015. TIGTA's Office of Investigations is involved in frequent conference calls with several IRS business units responsible for categorizing events, notifying potential victims of identity theft, and instituting digital blocks to

---

[8] The processes to verify someone is who he/she claims to be.
[9] The processes to determine the validity of evidence and the control over the evidence used to support a digital identity. Successful authentication provides reasonable risk-based assurances that the person accessing a service today is the same that previously accessed that service.
[10] Federation enables an identity provider (*i.e.*, a third party) to proof and authenticate an individual and provide identity assertions that the relying party (*e.g.*, the IRS) can accept and trust.

accounts when suspicious activity is detected. TIGTA has actively investigated a number of referrals of abnormalities and has verified that they were criminal activity of varying methods. Several of those methods exploited weaknesses that have since been closed.

The quality of findings produced by the IRS has increased and the timeliness of their interactions with TIGTA has improved. The CFAM group's reporting has recently become extremely useful and their findings more relevant and actionable. However, these efforts are largely driven by manual processes. The effectiveness of the CFAM group is limited and directly proportionate to the number of employees who can "look" at the data. The group also has not purchased Geolocation databases, which are very important when it comes to analyzing large Internet-based data sets.

TIGTA also identified concerns with the authentication of individuals submitting requests to the IRS. We evaluated IRS controls to authenticate requests received from individuals seeking to represent taxpayers and access taxpayer information and identified areas of improvement.[11] Taxpayers can grant a power of attorney to individuals (*i.e.*, representatives) who are given the authority to represent a taxpayer before the IRS. The representatives can be an attorney, certified public accountant, or enrolled agent.[12] Internal Revenue Code Section 6103(c) also allows taxpayers to authorize a designee to review and receive their returns and return information.

However, we found that IRS management has not implemented sufficient processes and procedures to authenticate the validity of Forms 2848, *Power of Attorney and Declaration of Representative*, and Forms 8821, *Taxpayer Information Authorization* that it receives. The IRS's reviews of these forms do not include steps to verify that the legitimate taxpayer submitted or signed the form to authorize access to his or her tax information. Based on the IRS's statistically valid sample, TIGTA estimates that the IRS has at least one unauthorized request form for 1.1 million taxpayers who have an authorization on file. In addition, the IRS did not protect 300 taxpayers after identifying that their Taxpayer Identification Numbers were obtained by fraudsters. The IRS should have used existing processes to monitor the use of Taxpayer Identification Numbers on future tax returns to identify potential identity theft.

---

[11] TIGTA, Ref. No. 2018-40-062, *Improved Procedures Are Needed to Prevent the Fraudulent Use of Third-Party Authorization Forms to Obtain Taxpayer Information* (Aug. 2018).
[12] The IRS enrolled agents program allows individuals to represent taxpayers before the IRS provided they have passed a three-part test and maintain continuing education requirements of 72 credit hours every three years.

Furthermore, we reported that the IRS has ineffective processes and procedures to ensure that legitimate taxpayers authorized the release of their tax transcript information to Income and Verification Express Services Program[13] participants or the participants' clients.[14] We recommended that the IRS implement processes and procedures to ensure that legitimate taxpayers authorized the release of their tax transcripts. We also recommended that the IRS discontinue offering tax transcripts via those processes in which the IRS cannot confirm whether legitimate taxpayers authorized the release of their tax transcripts.

In conclusion, expanded online access will increase the risk of unauthorized disclosure of taxpayer data. As such, the IRS's processes for authenticating individuals' identities must promote a high level of confidence that tax information and services are provided only to individuals who are entitled to receive them.

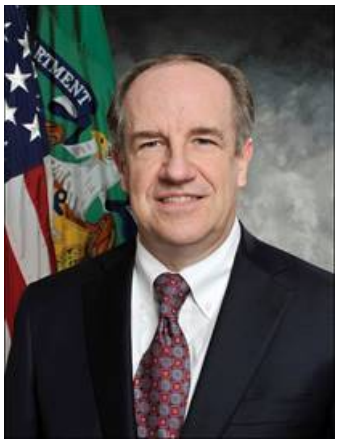
We at TIGTA take seriously our mandate to provide independent oversight of the IRS in its administration of our Nation's tax system. Accordingly, we plan to provide continuing audit coverage of the IRS's efforts to protect the confidentiality of taxpayer data.

Chairman Jenkins, Ranking Member Lewis, and Members of the Subcommittee, thank you for the opportunity to share my views.

---

[13] The Income and Verification Express Services Program is used by pre-screened companies who, in turn, are hired by clients such as mortgage firms and loan companies who need to verify applicants' income.

[14] TIGTA, Ref. No. 2018-40-014, *Transcript Delivery System Authentication and Authorization Processes Do Not Adequately Protect Against Unauthorized Release of Tax Information* (Mar. 2018).



Michael E. McKenney

Deputy Inspector General for Audit

Treasury Inspector General for Tax Administration

Mike McKenney serves as the Deputy Inspector General for Audit for the Treasury Inspector General for Tax Administration (TIGTA). He leads a nationwide audit function consisting of 267 staff members who strive to promote the economy, efficiency, and effectiveness of tax administration.

The Audit program's reports and recommendations to the Internal Revenue Service (IRS) have focused on improving tax administration and addressing the IRS's management challenges in the areas of data and employee security, computer modernization, tax law compliance and complexity, human capital, and improper and erroneous payments.

Previously, Mike served as the Assistant Inspector General for Audit (Returns Processing and Account Services) for TIGTA, where he was responsible for providing audit oversight of IRS operations related to the preparation and processing of tax returns and the issuing of refunds to taxpayers. This includes customer service activities, outreach efforts, tax law implementation, taxpayer assistance, accounts management, notices, submission processing, and upfront compliance such as the Frivolous Returns Program and the Questionable Refund Program.

Mike has served in various managerial positions with TIGTA, overseeing audits of a broad range of IRS programs including the IRS Oversight Board, Agency-Wide Shared Services, Chief Human Capital Office, Office of Appeals, Taxpayer Advocate Service, Office of Research and Analysis, and the Office of Professional Responsibility. Mike also opened and managed TIGTA's Denver field office for the Office of Audit. He began his Federal auditing career in 1992 with the IRS Inspection Service in Los Angeles. Mike graduated from California State University, Fullerton with a B.A. in Business (Accounting).