Hearing on the Internal Revenue Service's Taxpayer Online Authentication Efforts

---

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT

OF THE

COMMITTEE ON WAYS AND MEANS

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 26, 2018

Serial No. 115-OS14

COMMITTEE ON WAYS AND MEANS KEVIN BRADY, Texas, *Chairman*	
SAM JOHNSON, Texas DEVIN NUNES, California DAVID G. REICHERT, Washington PETER J. ROSKAM, Illinois VERN BUCHANAN, Florida ADRIAN SMITH, Nebraska LYNN JENKINS, Kansas ERIK PAULSEN, Minnesota KENNY MARCHANT, Texas DIANE BLACK, Tennessee TOM REED, New York MIKE KELLY, Pennsylvania JIM RENACCI, Ohio KRISTI NOEM, South Dakota GEORGE HOLDING, North Carolina JASON SMITH, Missouri TOM RICE, South Carolina DAVID SCHWEIKERT, Arizona JACKIE WALORSKI, Indiana CARLOS CURBELO, Florida MIKE BISHOP, Michigan DARIN LAHOOD, Illinois BRAD R. WENSTRUP, Ohio	RICHARD E. NEAL, Massachusetts SANDER M. LEVIN, Michigan JOHN LEWIS, Georgia LLOYD DOGGETT, Texas MIKE THOMPSON, California JOHN B. LARSON, Connecticut EARL BLUMENAUER, Oregon RON KIND, Wisconsin BILL PASCRELL, JR., New Jersey JOSEPH CROWLEY, New York DANNY DAVIS, Illinois LINDA SÁNCHEZ, California BRIAN HIGGINS, New York TERRI SEWELL, Alabama SUZAN DELBENE, Washington JUDY CHU, California
GARY ANDRES, *Staff Director* BRANDON CASEY, *Minority Chief Counsel*	

SUBCOMMITTEE ON OVERSIGHT LYNN JENKINS, Kansas, *Chairman*	
JACKIE WALORSKI, Indiana CARLOS CURBELO, Florida MIKE BISHOP, Michigan DARIN LAHOOD, Illinois BRAD R. WENSTRUP, Ohio KENNY MARCHANT, Texas	JOHN LEWIS, Georgia JOSEPH CROWLEY, New York SUZAN DELBENE, Washington EARL BLUMENAUER, Oregon

Hearing on the Internal Revenue Service's Taxpayer Authentication Efforts

U.S. House of Representatives,
Subcommittee on Oversight,
Committee on Ways and Means,
Washington, D.C

WITNESSES

Gina Garza
Chief Information Officer, IRS
Witness Statement

Edward Killen
Chief Privacy Officer, IRS
Witness Statement

James R. McTigue Jr.
Director, Tax Issues, Strategic Issues, Government Accountability Office (GAO)
Witness Statement

Michael McKenney
Deputy Inspector General for Audit, Treasury Inspector General for Tax Administration (TIGTA)
Witness Statement

WAYS AND MEANS
CHAIRMAN KEVIN BRADY

Chairman Jenkins Announces Hearing on the Internal Revenue Service's Taxpayer Online Authentication Efforts

House Ways and Means Oversight Subcommittee Chairman Lynn Jenkins (R-KS) announced today that the Subcommittee will hold a hearing entitled "IRS Taxpayer Authentication: Strengthening Security While Ensuring Access." The hearing will focus on how the IRS authenticates taxpayers using online tools and applications and addresses weaknesses in its authentication process. **The hearing will take place on Wednesday, September 26, 2018 in 2020 Rayburn House Office Building, beginning at 10:45 AM.**

In view of the limited time to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit written comments for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, http://waysandmeans.house.gov, select "Hearings." Select the hearing for which you would like to make a submission, and click on the link entitled, "Click here to provide a submission for the record." Once you have followed the online instructions, submit all requested information. ATTACH your submission as a Word document, in compliance with the formatting requirements listed below, **by the close of business on Wednesday October 10, 2018.** For questions, or if you encounter technical problems, please call (202) 225-3625.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any materials submitted for the printed record, and any written

comments in response to a request for written comments must conform to the guidelines listed below. Any submission not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

All submissions and supplementary materials must be submitted in a single document via email, provided in Word format and must not exceed a total of 10 pages. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.

All submissions must include a list of all clients, persons and/or organizations on whose behalf the witness appears. The name, company, address, telephone, and fax numbers of each witness must be included in the body of the email. Please exclude any personal identifiable information in the attached submission.

Failure to follow the formatting requirements may result in the exclusion of a submission. All submissions for the record are final.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202-225-1721 or 202-226-3411 TTD/TTY in advance of the event (four business days' notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Note: All Committee advisories and news releases are available at http://www.waysandmeans.house.gov/

THE INTERNAL REVENUE SERVICE'S

TAXPAYER ONLINE AUTHENTICATION EFFORTS

Wednesday, September 26, 2018

House of Representatives,

Subcommittee on Oversight,

Committee on Ways and Means,

Washington, D.C.

The Subcommittee met, pursuant to notice, at 10:46 a.m., in Room 2020, Rayburn House Office Building, Hon. Lynn Jenkins [Chairman of the Subcommittee] presiding.

*Chairman Jenkins. Good morning. The Subcommittee will come to order. Welcome to the Ways and Means Oversight Subcommittee hearing on "IRS Taxpayer Authentication: Strengthening Security While Ensuring Access" hearing.

Last year, taxpayers and third parties electronically completed more than 330 million transactions with the IRS. To do so, taxpayers used a number of online tools and applications, which offer convenient ways to interact with the IRS. These tools and applications allow taxpayers to make payments to the IRS, check the status of their refunds, and review prior year return information instead of having to call the IRS or visit an IRS office.

Sadly, the IRS's online tools and applications have also become an attractive target for criminals looking to steal taxpayer information and commit identity theft fraud. The IRS uses a process known as "authentication" to separate legitimate taxpayers who want to access the IRS's online services from criminals looking to commit fraud. Unfortunately, given the large amount of personal information on taxpayers available in the public domain, criminals can easily impersonate legitimate taxpayers and pass through the IRS's authentication process undetected.

To combat this problem, the IRS needs to ensure the necessary layers of defense are in place when authenticating taxpayers.

However, both the Government Accountability Office and the Treasury Inspector General for Tax Administration have raised concerns with how the IRS authenticates users of its online tools and applications. For example, the IRS only required limited authentication of two key online applications, even though federal guidelines recommended more robust efforts. Subsequent breaches of these applications in 2015 and 2016 exposed taxpayers to the harm of identity theft.

For its part, the IRS has tried to improve its online authentication through multiple efforts. Unfortunately, the IRS has not implemented a comprehensive authentication strategy to coordinate these efforts, even though it has been working on one for nearly three years. Without a strategy in place, the IRS will not be able to establish an agency-wide response to improve authentication.

Congress also recognizes the importance of establishing secure channels for taxpayers to interact with the IRS online. Last April, the House of Representatives passed the Taxpayer First Act, which establishes a framework for the IRS to develop effective online tools and applications that protect taxpayer information.

Today's hearing will focus on the IRS's current online authentication efforts; the challenges the IRS faces when authenticating taxpayers online; and the areas where the IRS can improve its authentication efforts.

As criminals continue to evolve and become more sophisticated in their attacks, finding the appropriate solutions for authenticating taxpayers becomes all the more important.

The IRS should also consider balancing the appropriate level of authentication while ensuring legitimate taxpayers are able to access online services.

*Chairman Jenkins. I want to thank our witnesses for being here today, and we look forward to their testimony.

We will yield to the Ranking Member, Mr. Lewis, when he arrives, for the purpose of his opening statement.

But with that, I think we will go ahead and hear from our witnesses. Today's witness panel includes four experts: Gina Garza, Chief Information Officer at the Internal Revenue Service; Edward Killen, Chief Privacy Officer at the Internal Revenue Service; James McTigue, Director of Tax Issues at the Government Accountability Office; Mike McKenney, Deputy Inspector General for Audit at the Treasury Inspector General for Tax Administration.

This Subcommittee has received your written statements, and they will be able to be made part of the formal hearing record. You will each have five minutes to deliver your opening statements.

But the Ranking Member has arrived, and I would love to yield to our Distinguished Ranking Member, Mr. Lewis, for purposes of an opening statement.

Good morning.

*Mr. Lewis. Good morning, Madam Chair. I regret that I am running late.

*Chairman Jenkins. No worries. You are kind of busy. It is a busy week.

*Mr. Lewis. Well, we all are busy these days, you know? It is a busy time.

Good morning, everybody. You are a good-looking group. You look very smart. And thank you so much for being here.

Madam Chair, since I am running so late, and I don't want to take up time, I will be very brief. I will not read my entire statement. My staff people won't be pleased with -- you know, sometimes I cannot please them.

[Laughter.]

*Mr. Lewis. Madam Chair, thank you for holding this hearing. I would also like to thank our witnesses for being here this morning.

Today's hearing will examine how the Internal Revenue Service confirms taxpayers' identities when they use online services. This process is important for reducing identity theft and refund fraud. The growing number of security breaches across the public and private sector often make it difficult for the agency to verify the real taxpayer.

In many cases, criminals combine sensitive taxpayer information that they stole from several sources. The thieves use this information to access a taxpayer's online account, or file a fraudulent tax return. The impact of these tactics is severe and costly.

For example, criminals stole more than $1.5 billion by filing fraudulent tax refunds in 2016. Just last year, the IRS shut down a popular online service that students use to apply for federal financial aid after a breach allowed crooks to access the adjusted gross income of about 100,000 taxpayers.

We can do better. We must do better. With the necessary resources, we will all do better.

*Mr. Lewis. And again, Madam Chair, thank you for holding this hearing. I look forward to the testimony of our witnesses, and I yield back. Thank you.

*Chairman Jenkins. Thank you, Mr. Lewis. And without objection, other Members' opening statements will be made part of the record.

I understand Ms. Garza is here as a supporting role, will be taking our questions, but does not have a formal testimony to offer, initially. So we will begin with Mr. Killen.

You may begin when you are ready.

OPENING STATEMENT OF CONGRESSMAN JOHN LEWIS (D-GA)
COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON OVERSIGHT
HEARING ON
INTERNAL REVENUE SERVICE'S TAXPAYER ONLINE AUTHENTICATION EFFORTS
September 26, 2018

Madam Chair, thank you for holding this hearing. I would also like to thank our witnesses for being here this morning.

Today's hearing will examine how the Internal Revenue Service confirms taxpayers identities when they use online services. This process is important for reducing identity theft and refund fraud.

The growing number of security breaches across the public and private sectors often make it difficult for the agency to verify the real taxpayer. In many cases, criminals combine sensitive taxpayer information that they stole from several sources. The thieves use this information to access a taxpayer's online account or file a fraudulent tax return.

The impact of these tactics are severe and costly. For example, criminals stole more than $1.5 billion by filing fraudulent tax refunds in 2016. Just last year, the IRS shut down a popular online service that students use to apply for federal financial aid after a breach allowed crooks to access the adjusted gross income of about 100,000 taxpayers.

Madam Chair, we all agree that the IRS is making progress. I applaud the agency for reducing tax-related identity theft. I am also pleased that agency officials partnered with industry and States to protect taxpayers and reduce identity theft.

Although I am encouraged that the agency improved its efforts to protect taxpayer data, the IRS must keep up the fight. As online services become more popular, there will be additional pressure to detect and stop security threats before the criminals reap the rewards.

In closing, I must note the relationship between resources and the security and protection of taxpayers. The IRS must have adequate funding in order to provide online services, computer systems, and technology that can withstand an average of 2.5 million cyberattacks each and every day. Since 2010, Congress cut this agency's budget by almost $1 billion. Many of you heard me say it many times—you cannot get blood from a turnip. Together, we must and we can do more.

Madam Chair, I hope that we will continue our bipartisan work on this issue. Again, I thank you for holding this hearing, and I look forward to the witnesses' testimony.

STATEMENT OF EDWARD KILLEN, CHIEF PRIVACY OFFICER, IRS

*Mr. Killen. Good morning. Chairman Jenkins, Ranking Member Lewis, and Members of the Subcommittee, my name is Edward Killen, and I am the chief privacy officer of the IRS. With me today is Gina Garza, the IRS's chief information officer. We appreciate the opportunity to testify today.

In my role at the IRS I represent the agency's interest in several areas, including privacy compliance, information protection, records management, disclosure, and data sharing.

In addition, approximately four months ago, in May 2018, I became responsible for the access and authentication strategy. Testifying with me today is Gina Garza, and Gina's role -- she is responsible for all aspects of our systems that operate the Nation's tax infrastructure, and support the processing of 200 million tax returns, annually. We share large aspects of the responsibility for protecting the privacy and security of taxpayer data.

We also partner to provide taxpayers and their authorized representatives secure and expanded online access to meet their tax obligations. Our testimony today will reflect that partnership.

Protecting taxpayers and their data is not just the job of our offices, it is a foundational priority across the IRS, and an extremely important aspect of taxpayer service.

The IRS works to protect taxpayers in two primary ways. First, we work continuously to safeguard our computer systems from cyber incidents, intrusions, and attacks. Our systems currently withstand an average of 2.5 million intrusion attempts daily. Some of these attempts are sophisticated in nature, or represent advanced, persistent threats.

Second, the IRS is waging an ongoing battle to protect taxpayer information. This effort is complicated by the vast amounts of data available to fraudsters from public and private-sector breaches outside the tax system. This information can be used to exploit weak authentication protocols and perpetrate all types of fraudulent activity, including tax refund fraud.

To address this problem, we are leveraging our security relationships to develop multi-layer defenses against fraudsters. As a result of the collective efforts, we have been able to reduce the number of tax returns with confirmed identity theft by 57 percent, with more than $20 billion in taxpayer refunds protected.

While we have made significant progress combating tax-related identity theft, we must remain vigilant. Cyber criminals are growing in sophistication, and they are constantly working to find new ways to steal taxpayer data and file fraudulent tax returns. The implementation of appropriate and effective authentication protocols is a key armament in the war against these fraudsters.

The IRS took an initial step toward effective protocols when we issued our "Identity Assurance Strategy and Roadmap" in 2016, a document designed to identify both short and long-term needs to strengthen the IRS's identity assurance posture.

To be successful, our strategy requires a three-pronged approach that considers relevant policies, information technology capabilities, and operational needs. We are implementing the strategy, strengthening online authentication protocols, and fortifying our defenses.

Another important step was implementing the Secure Access e-authentication system in 2016. This is a rigorous process that helps protect the IRS's online tools in two ways. First, it has a strong identity-proofing procedure to establish that first-time users are who they say they are. Second, it requires returning users to go through a two-factor process to authenticate their identity. These are only two of the many important activities in our ongoing work to protect taxpayers from evolving data threats, while meeting increasing taxpayer expectations for online access and tools.

We recognize that we have much more work to do, and we are committed to doing that work.

Chairman Jenkins, Ranking Member Lewis, and Members of the Subcommittee, this concludes our joint statement. Gina and I will be happy to take your questions.

WRITTEN TESTIMONY OF
EDWARD T. KILLEN
CHIEF PRIVACY OFFICER
AND
SILVANA GINA GARZA
CHIEF INFORMATION OFFICER
INTERNAL REVENUE SERVICE
BEFORE THE
HOUSE WAYS AND MEANS COMMITTEE
SUBCOMMITTEE ON OVERSIGHT
ON IRS TAXPAYER AUTHENTICATION EFFORTS
SEPTEMBER 26, 2018

INTRODUCTION

Chairman Jenkins, Ranking Member Lewis, and Members of the Subcommittee, thank you for the opportunity to discuss the IRS's taxpayer authentication processes as they support our overall data protection efforts.

Securing our systems and taxpayer data continues to be a top priority for the IRS. First, the IRS works continuously to protect our computer systems from cyber incidents, intrusions and attacks. They remain secure through a combination of cyber defenses, which currently withstand about an average of 2 ½ million attempts a day to access our systems. Many of these attempts are sophisticated in nature or represent advanced persistent threats. Second, the IRS is waging an ongoing battle to protect taxpayers and their information against the growing problem of identity theft, particularly tax refund fraud, for which cybercriminals frequently exploit vast amounts of data from breaches outside the tax system.

One of the critical components of the IRS's efforts to secure our systems and protect taxpayer data involves continuously working to improve our processes for authenticating the identities of taxpayers who interact with the agency through our service channels, including in-person, over the phone and online. Over the last several years, we particularly focused on strengthening our online authentication processes, and we have made critical progress in this area.

However, the cyber landscape is ever changing. Efforts to steal taxpayer data and infiltrate our systems, by cybercriminals with access to cutting-edge technology, resources and new methods, continue to grow in sophistication, frequency, brazenness, volume and impact. As a result, the risks associated with sophisticated cybersecurity threats are increasing. This is confirmed by the growing incidence of cybercrime (theft by unauthorized access) and privacy breaches we are seeing across the country in all areas of government and

industry. Remaining current with the latest technologies, processes and counter-measures will continue to challenge the IRS, but we will work diligently to strengthen data protections as we expand online services and applications for taxpayers.

SAFEGUARDING IRS SYSTEMS AND TAXPAYER DATA

The IRS has made significant progress over the last several years in protecting taxpayers and the tax system against tax-related identity theft. A major contributor to this progress is the work being done by the Security Summit, a unique partnership that includes the IRS, tax industry leaders and state tax commissioners. This partnership, in combination with our fraud detection systems, is making a difference. In fact, the 2018 filing season was the third in which the IRS worked with our Security Summit partners to put in place many protections to help stop fraudulent returns from entering tax processing systems.

I'm pleased to report recent statistics show a continuing and substantial decline in several indicators of tax-related identity theft. From 2015 to 2017, the number of taxpayers reporting to the IRS that they were victims of identity theft dropped by 65 percent, and the number of tax returns with confirmed identity theft fell by 57 percent with more than $20 billion in taxpayer refunds being protected.

An important part of the Summit's work has involved sharing information, especially leads on emerging identity theft schemes. Toward that end, in 2017 the Summit partners created the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC), which has helped Summit partners to rapidly share information and the IRS to identify emerging schemes. Sharing information and doing it in a timely manner is critical to our ability to respond rapidly to evolving threats, so the ISAC will be an important tool going forward.

We realize we cannot let up in the fight against fraud and tax-related identity theft. As we have strengthened our defenses, identity thieves are continuously working to obtain more-detailed financial information to help them do a better job of impersonating legitimate taxpayers and file more realistic-looking tax returns to claim fraudulent refunds.

Cyberthieves are targeting tax professionals, human resources departments, businesses and other places with large amounts of sensitive financial information. Therefore, the IRS and its partners not only continue to improve our safeguards against fraudulent returns, but we also continue to encourage taxpayers, tax professionals and businesses to protect their data and avoid becoming victims of proliferating tax scams.

AUTHENTICATION PROCEDURES AND ONGOING IMPROVEMENTS

A major component of the IRS's efforts to protect taxpayer data and combat cyber fraud and tax-related identity theft involves our authentication procedures for online transactions. The IRS makes every effort to ensure that we provide tax account-related services only after verifying the identity of individuals seeking those services – whether this inquiry is on-line, in-person, or via telephone. For the last several years, we have been working to improve our authentication processes and procedures, including the development of a strong, coordinated and evolving authentication framework.

In 2015, the IRS established the Identity Assurance Office to help us better understand authentication and fraud detection needs across the agency. The following year, the Identity Assurance Office issued its IRS Identity Assurance Strategy and Roadmap. The Strategy and Roadmap includes core objectives, priority campaigns and foundational initiatives designed to meet both short- and long-term needs to strengthen the IRS's identity assurance posture. This guiding document has been essential in putting the IRS on a path to more robust omni-channel taxpayer authentication procedures, online capabilities and services. As this field continues to evolve dynamically, with the pace of technological changes and the risks associated with sophisticated cybersecurity threats, we will continue to update this document to ensure it addresses current IRS needs and reflects state-of-the-art technological capabilities and evolving federal requirements.

Secure Access System

The IRS employs differing Levels of Assurance among the various digital services used by taxpayers, according to the risk involved. For example, the level of assurance required for an online tool that only accepts payments from a taxpayer can reasonably be set lower than an application that provides taxpayers access to their personal tax information.

The IRS took an important step forward in safeguarding high-risk transactions in 2016 when it implemented the Secure Access e-Authentication system, a rigorous identity verification process that helps protect the IRS's online tools in two ways. First, it has a strong identity-proofing process, which helps establish that first-time users are who they say they are. Second, it requires returning users to authenticate and go through a two-factor access process by entering their username and password plus a security code. The security code can be sent via text message to their mobile phone, or as a more secure option, can be generated by the IRS2Go mobile app. This two-factor authentication process met the federal standards for protecting information that were recently superseded by the new National Institute of Standards and Technology (NIST) guidelines. We are now evaluating how to comply with the new standards (NIST 800-63-3), as we explain in greater detail below.

Overall, the IRS takes a risk-based approach to evaluating the level of security required based on federal guidelines. Since implementing Secure Access, the IRS has analyzed each online application we offer to taxpayers and tax professionals, and the types of transactions those applications enable, to identify the applications that require the highest levels of authentication.

The first applications we migrated to Secure Access were the most critical services and applications – ones that provide users with sensitive information. Those include, for example, obtaining prior-year tax information using the Get Transcript Online application, looking up an Identity Protection Personal Identification Number, and accessing the taxpayer's online IRS account. We have continued to migrate other online tools to the Secure Access system as appropriate. We took a major step in December 2017 when we extended Secure Access protections to e-Services, which is a suite of online tools for tax professionals, including electronic filing, transcript delivery systems and taxpayer identification number matching. This was especially important because these tools access sensitive data, and because cybercriminals increasingly target tax professionals.

The IRS will continue to look carefully at how taxpayers interact with our online web applications and make improvements where needed. This focus on the user experience applies not only to online applications, but also to other service channels where the IRS continues to hear the voice of the customer to drive service improvements.

OMB and NIST Standards

The IRS is committed to continuously improving our authentication procedures in line with guidelines from the Office of Management and Budget (OMB) and NIST, which apply to all federal agencies implementing digital identity services. Over the past year, the IRS performed an in-depth analysis of all its secure online applications used by taxpayers and tax professionals. Our goal was to ensure we employed adequate security controls. Where necessary, we implemented strong mitigations and compensating controls to strengthen the overall security of online services. Through our analysis, we confirmed that applications behind Secure Access were fully compliant with the guidelines outlined in NIST Special Publication (SP) 800-63-2.

As noted above, NIST revised its guidelines in June 2017 with the release of NIST SP 800-63-3. This was a complete rewrite of the eAuthentication standard, and creates a new framework for federal agencies to improve the security of their identity-proofing and authentication programs. The new guidelines introduce new concepts and redefine how federal agencies implement digital identity services. Further, the new standard has substantially more rigorous requirements than the previous standard. The IRS is working to assess how the new guidelines affect the processes and systems that taxpayers use, and we have taken preliminary

steps to implement the guidelines. For example, we developed a comprehensive, data-driven approach to assess applications against the new NIST guidelines and have begun testing the new process.

One of the first steps we took was to determine the extent to which existing applications might meet the new NIST standards. For example, we assessed the current Secure Access system against the new NIST guidelines. We found the IRS meets Authentication Assurance Level (AAL) 2 and Identity Assurance Level (IAL) 1 requirements. However, like all federal agencies, the IRS faces challenges implementing the new NIST standards. As they enter the market, new products and services must be certified by the appropriate credentialing authorities. We understand that this work is ongoing. In effect, commercially-available solutions that meet the new, more stringent requirements are not yet widely available. Despite these challenges, the IRS continues to pursue a secure digital experience for all users.

Monitoring Suspicious Activity

Another aspect of ensuring that only authorized users access taxpayer data in our systems involves our efforts to monitor, detect and analyze suspicious activity in those systems. As the IRS has improved its procedures for authenticating users of our online services, we have also enhanced network monitoring controls to help block suspicious activity on IRS.gov, and thus thwart cybercriminals' attempts to obtain unauthorized access to taxpayer data through our online applications. However, the cyber landscape is consistently shifting, requiring stronger authentication requirements and robust cyber monitoring tools; which has increased costs for programs.

In a report earlier this year, the Treasury Inspector General for Tax Administration (TIGTA) noted that the IRS has made progress toward implementing effective network monitoring controls, and the controls now in place provide a significant improvement in the IRS's ability to detect and prevent cyberattacks. At the same time, we acknowledge that the IRS has more work to do in this area. We agree with all of the recommendations for improvement TIGTA made in its report and are working to address each one.

Chairman Jenkins, Ranking Member Lewis and Members of the Subcommittee, this concludes my statement. I would be happy to take your questions.

*Chairman Jenkins. Thank you, Mr. Killen.

Mr. McTigue, we will turn to you.

STATEMENT OF JAMES R. MCTIGUE JR., DIRECTOR, TAX ISSUES, STRATEGIC ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE (GAO)

*Mr. McTigue. Chairman Jenkins, Ranking Member Lewis, and Members of the Subcommittee, I am pleased to be here today to discuss the Internal Revenue Service's efforts to improve taxpayer authentication.

IRS's mission is to provide taxpayers with quality service and help them meet their tax-filing responsibilities. In doing so, it is critically important that it protects sensitive taxpayer information and avoids paying, potentially, billions of dollars in fraudulent refunds each year.

One of the key ways it can do this is through authentication, the process by which it verifies that taxpayers are who they claim to be online, on the phone, through the mail, or in person.

My remarks today highlight selected findings of our June 2018 report. In particular, I will describe IRS's efforts to address its authentication challenges, IRS's progress in implementing its authentication strategy, and finally, additional steps that IRS could take to enhance its authentication programs.

First, IRS has established organizational structures essential to supporting its taxpayer authentication efforts. Specifically, IRS created the identity assurance office in 2015 to work with stakeholders across the service to mitigate risk in all authentication programs and service delivery channels. In fact, the office cataloged over 100 types of interactions between IRS and taxpayers that require authentication.

Based on this and other efforts, in December 2016 IRS released the comprehensive strategy for developing a modern and secure authentication environment that both increases security and improves customer access.

IRS has also been collaborating with industry and state partners via the Security Summit to address common authentication challenges. For example, the Security Summit's authentication working group identified key data elements embedded in electronically-filed tax returns that have helped provide IRS with greater assurance that a filed tax return is legitimate.

Second, although IRS is going to implement its authentication strategy, it has not prioritized initiatives nor established the resources required to support its strategy, which would be consistent with leading program management practices.

We recognize that a strategy is necessarily high level, and IRS must remain flexible and use available resources to respond to unexpected threats. However, if IRS estimated resource requirements and prioritized activities, it would be better able to clarify tradeoffs between cost, benefits, and risks of different activities, allowing it to make more informed decisions.

Third, given the widespread availability of personally-identifiable information, it is essential that IRS continuously strengthen taxpayer authentication to stay ahead of fraudsters without overly burdening taxpayers. As such, we highlighted two areas that IRS must address.

First, IRS has not yet established detailed plans with timelines and resources needed to fully implement the June 2017 guidelines from the National Institute of Standards and Technology, or NIST, for secure online authentication. NIST calls for federal agencies to conduct a risk assessment for each component of identity assurance: identity proofing, authentication, and federation. Such an assessment would help ensure IRS that it is selecting the right level of security for each taxpayer interaction.

Second, IRS lacks a continuous process for identifying and evaluating potential new authentication approaches, such as possession-based authentication using security key-type devices. Other examples include working with trusted partners, such as tax preparers, financial institutions, or other federal or state agencies.

And also, expanding the functionality of its online account to send taxpayers notifications by text, email, or the IRS2Go app when there is activity on their account, which could help stop fraudsters steal refunds [sic].

With this in mind, GAO made 11 recommendations focused on four areas.

First, it needs to estimate resources for and prioritize its authentication initiatives.

Second, it needs to complete risk assessments, improve monitoring of telephone, in-person, and correspondence authentication.

Third, it needs to develop a plan to fully implement the new NIST guidance on secure digital authentication.

And fourth, IRS needs to implement a process to regularly identify and evaluate potential new authentication approaches.

IRS agreed with all 11 of our recommendations, and has plans to begin implementing them. Addressing these issues will better position IRS to protect taxpayers and the Treasury.

Chairman Jenkins, Ranking Member Lewis, and Members of the Subcommittee, that concludes my prepared remarks, and I look forward to your questions.

United States Government Accountability Office

Testimony

Before the Subcommittee on Oversight, Committee on Ways and Means, House of Representatives

For Release on Delivery
Expected at 10:45 a.m.
Wednesday, September 26, 2018

IDENTITY THEFT

Strengthening Taxpayer Authentication Efforts Could Help Protect IRS Against Fraudsters

Statement of James R. McTigue, Jr., Director, Strategic Issues

Chairman Jenkins, Ranking Member Lewis, and Members of the Subcommittee:

I am pleased to be here today to discuss the Internal Revenue Service's (IRS) efforts to monitor and improve taxpayer authentication. In fiscal year 2017, IRS issued approximately $383 billion in individual tax refunds, including overpayment refunds and refundable tax credits, an increase of about $16 billion from the previous fiscal year. In an environment with an increasing risk of fraud, identity theft (IDT), and cyberattacks, IRS must ensure that its preventative security controls provide the agency with reasonable assurance that it is interacting with the legitimate taxpayer. Authentication—the process by which IRS verifies taxpayers are who they claim to be—is a critical step in both protecting sensitive taxpayer information and preventing potentially billions of dollars of refunds from being paid to fraudsters each year. According to IRS's most recent data, it estimates that in 2016, at least $12.2 billion in IDT tax refund fraud was attempted; of this amount, at least $1.6 billion was paid out to fraudsters.

IRS's ability to continuously monitor its current authentication methods while also looking ahead to new identity verification technologies is critical to keeping ahead of fraudsters, who constantly adapt their schemes to thwart IRS's defenses. The agency must also strike a balance in designing its authentication programs. Authentication must be strong enough to prevent fraudsters from gaining access to IRS services using stolen personally identifiable information, without being overly burdensome on legitimate taxpayers who also must authenticate.

My remarks today highlight selected findings of our June 2018 report on IRS's efforts monitor and improve taxpayer authentication.[1] Specifically, this testimony addresses (1) IRS's efforts to address its authentication challenges, (2) IRS's progress in implementing its authentication strategy, and (3) additional steps we identified that IRS could take to enhance its authentication programs and stay ahead of fraudsters.

To conduct the work for our June report, we reviewed IRS documents and information related to taxpayer authentication including authentication policies, risk assessments, and performance metrics. We compared IRS's authentication efforts to applicable activities in the *IRS Identity Assurance*

[1]GAO, *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts,* GAO-18-418 (Washington, D.C.: June 22, 2018).

Strategy and Roadmap (Roadmap), Standards for Internal Control in the Federal Government, and relevant National Institute of Standards and Technology (NIST) guidance, among others.[2] We also interviewed IRS officials knowledgeable about the agency's taxpayer authentication programs, as well as IRS, state, and industry co-leads from two Security Summit workgroups to understand IRS's collaborative efforts to improve taxpayer authentication.[3] To assess how IRS can improve its authentication programs going forward, we met with knowledgeable officials from NIST to discuss its guidelines for online identity-proofing and authentication. We also compared IRS's authentication programs and plans for future improvements to its *Roadmap*, federal internal controls, guidance from NIST and the Office of Management and Budget (OMB), principles for project planning, and our prior work on information technology investment management and cost estimating. We also interviewed officials from three other federal agencies and a nongeneralizable selection of representatives from state revenue offices, industry, and financial institutions to understand the range of authentication technologies other organizations are using. Our report includes a detailed explanation of the methods used to conduct our work. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

In brief, Madam Chairman, our work found that IRS has taken some steps to improve taxpayer authentication, including working with external partners to identify solutions for combating IDT refund fraud and developing an authentication strategy to address its most pressing authentication challenges. However, we also found that IRS has not prioritized the initiatives supporting its authentication strategy nor identified the resources required to complete them. Further, we found that IRS does not have clear plans and timelines to fully implement NIST's new guidance for secure online authentication and also lacks a comprehensive process to evaluate potential new authentication technologies, which could provide taxpayers additional options to actively

[2]GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: September 2014); and *A Framework for Managing Fraud Risks in Federal Programs,* GAO-15-593SP (Washington, D.C.: July 28, 2015). National Institute of Standards and Technology, *Electronic Authentication Guideline*, *Special Publication 800-63-2,* (August 2013), superseded by *Digital Identity Guidelines, Special Publication 800-63-3* (June 2017).

[3]The Security Summit is an ongoing effort between IRS, industry and states to address IDT challenges.

protect their identity. We made 11 recommendations to address these and other weaknesses identified in our report. IRS agreed with all 11 recommendations and stated that it is taking action to address them.

IRS Has Broad Efforts Underway to Address Authentication Challenges

Our report noted that IRS has established organizational structures essential to supporting its taxpayer authentication efforts. Specifically, IRS created an Identity Assurance Office (IAO) in 2015 to work with stakeholders across IRS to review and assess the agency's various authentication programs and efforts. In 2016, IAO led an effort that identified over 100 interactions between IRS and taxpayers that require authentication and categorized these interactions based on potential risks to the agency and taxpayers. Further, in December 2016, IAO released its *Roadmap* for developing a modern and secure authentication environment for all taxpayers regardless of how they interact with IRS—online, over the telephone, in person, or via correspondence.

We also found that IRS is working to address its authentication challenges by collaborating with industry members and state partners via the Security Summit. The Security Summit was established in 2015 as an ongoing effort between industry experts from tax software companies, paid preparers, financial institutions, and states to improve information sharing and fraud detection and to address common IDT challenges. The Security Summit's authentication workgroup leads several initiatives aimed at verifying the authenticity of the taxpayer and the tax return at the time of filing. One initiative involves analyzing data elements—such as trusted customer requirements and other characteristics of the return—that are collected during the tax return preparation and electronic filing process. In addition, in 2016 the authentication workgroup recommended improved account password standards to help protect taxpayers' accounts from being taken over by criminals.

Overall, we found that officials—representing IRS, industry, and states—expressed positive views about the level of commitment and cooperation guiding the group's authentication efforts. Officials with whom we spoke stated that they are dedicated to continuing to address authentication issues collaboratively because they have a mutual interest in improving authentication to reduce tax refund fraud.

IRS Has Begun to Implement Its Authentication Strategy, but Has Not Articulated Priorities and Resource Needs

In its *Roadmap*, IRS outlined six core authentication objectives, 10 high-level strategic efforts, and 14 foundational initiatives to help it address authentication challenges and identify opportunities for future investment. While we found that IRS has made progress on some efforts identified in its *Roadmap*, it has not prioritized the initiatives supporting its strategy nor identified the resources required to complete them, consistent with program management leading practices.

For example, one of IRS's foundational initiatives is to send event-driven notifications to taxpayers, such as when they file a return or request a tax transcript. Such notifications could help IRS and taxpayers detect potentially fraudulent activity at the earliest stage and help improve authentication of tax returns. The *Roadmap* identifies seven supporting activities for this foundational initiative. One is to provide taxpayers with greater control over their online accounts. Another supporting activity is to determine methods for sending notifications to taxpayers about activity on their account.[4]

However, IRS has not identified the resources required to complete these activities, and the *Roadmap* notes that six of the seven activities will take between 6 months to 3 years to complete. In December 2017, IRS officials stated that they had developed business requirements for the foundational initiative to give taxpayers greater control over their online accounts. However, IRS has not identified funding for the initiative's other supporting activities—such as developing requirements to send push notifications to taxpayers—and implementation will depend on the availability of future resources.[5]

In December 2017, IRS officials stated that each of the strategic efforts and foundational initiatives identified in the *Roadmap* are a high priority, and they are working to address them concurrently while balancing the availability of resources against the greatest threats to the tax environment. As noted in our report, we recognize that a strategy is necessarily high-level and that IRS must remain flexible and use available

[4]According to IRS, notifications could be sent to the taxpayer via the IRS2Go application, text message, or e-mail. For example, the message could alert the taxpayer that a tax return was filed using the social security number associated with their online account.

[5]In January 2018, IRS officials noted that although this type of alert is not currently available, taxpayers can access their online account to review whether a return has been processed and filed for a current or prior tax year.

resources to respond to unexpected threats. Identifying resources and prioritizing activities in its *Roadmap* will help IRS clarify tradeoffs between costs, benefits, and risks and aid in decision making.

Further, such efforts may also help IRS establish clearer timelines and better respond to unexpected events. As such, we recommended that IRS estimate the resources (i.e., financial and human) required for the foundational initiatives and supporting activities identified in its *Roadmap* and prioritize its foundational initiatives. IRS agreed with our recommendations and is currently working to finalize its overall authentication approach.

Additional Actions Could Help IRS Enhance Security and Stay Ahead of Fraudsters

Given the widespread availability of personally identifiable information that fraudsters can use to perpetrate tax fraud, it is essential for IRS to further strengthen taxpayer authentication to stay ahead of fraudsters' schemes. In our report, we identified two additional areas that IRS must address to better position the agency and protect taxpayers against future threats.

First, we found that IRS has taken preliminary steps to implement NIST's June 2017 guidance for secure online authentication, however it had not yet established detailed plans, including timelines, milestone dates, and resource needs to fully implement it. Among other things, NIST's new guidance directs agencies to assess the risk for each component of identity assurance—identity proofing, authentication, and federation—rather than conducting a single risk assessment for the entire process.[6] According to NIST officials, this approach gives agencies flexibility in choosing technical solutions; aligns with existing, standards-based market offerings; is modular and cost-effective; and enhances individual privacy. In short, following NIST's new guidance will help provide IRS with better risk-based assurance that the person trying to access IRS's online services is who they claim to be.

As noted in our report, IRS has taken preliminary steps to implement the new NIST guidance. These efforts include forming a task force to guide IRS's implementation of NIST guidance and working with the Security

[6]According to NIST, identity proofing establishes that the person is actually who they claim to be; authentication verifies that the person attempting to access a service is in control of one or more valid authenticators associated with that person's identity; and federation is the concept that one set of user credentials can be used to access multiple systems.

Summit to develop an implementation framework for state and industry partners. IRS has also begun analyzing gaps between IRS's current authentication procedures and the new guidance. In addition, in December 2017, IRS implemented a more secure online authentication option consistent with the new guidance through its mobile application, IRS2Go. After taxpayers link their IRS online account with the mobile app, they can use it to generate a security code to log into their account. This option provides taxpayers with an alternative to receiving the security code via a text message, which NIST considers to be less secure.

We recommended that IRS develop a plan—including a timeline, milestone dates, and resources needed—for implementing changes to its online authentication programs consistent with new NIST guidance, and also implement these improvements. IRS agreed with our recommendations, but noted that its ability to complete these efforts will depend on the availability of resources.

Second, we found that IRS lacks a comprehensive, repeatable process to identify and evaluate potential new authentication technologies and approaches. Our discussions with representatives from industry and financial institutions and with government officials indicate that there is no single, ideal online authentication solution that will solve IRS's challenges related to IDT refund fraud. These representatives advocate an approach to authentication that relies on multiple strategies and sources of information, while giving taxpayers options for further protecting their information.

We identified several authentication options in our report that IRS could consider, including the following:

- **Possession-based authentication.** This type of authentication offers users a convenient, added layer of security when used as a second factor for accessing websites or systems that would otherwise rely on a username and password for single-factor authentication. For example, as noted in our report, according to an industry official, authentication using a trusted device or "security key" based on Universal Second Factor standards complies with NIST's new guidance for digital authentication. While IRS is not likely to provide the devices to taxpayers, it could enable its systems to accept these trusted devices as authenticators for taxpayers who elect to use them.
- **Working with trusted partners.** IRS could partner with organizations it trusts that are accessible to taxpayers and enable the partners to identity-proof and authenticate taxpayers. Trusted partners could

include tax preparers, financial institutions, or other federal or state agencies. In the course of our work, IRS officials stated that they had been exploring such options with both the Social Security Administration and the U.S. Postal Service; however, at the time of our report, the agencies had not yet made decisions about next steps.

- **Expanding existing IRS services to further protect taxpayers.** IRS could expand the functionality of its online account to further protect taxpayers from IDT refund fraud. For example, IRS could develop additional functionality that allows the taxpayer to designate a bank account or a preference for a paper check for receiving a tax refund. If a fraudster filed a return with different information, the return would be automatically rejected.

IRS officials told us the agency continually researches new identity assurance processes and technologies and has talked with other agencies, industry groups, and vendors to better understand how particular technology solutions could apply to IRS's environment. However, during the course of our work, IRS could not provide us evidence of a repeatable, comprehensive process to identify and evaluate available authentication technologies and services. Such a process could compare options for in-house authentication solutions with off-the-shelf solutions based on estimates of cost, schedule, and benefits, as applicable. To this end, we recommended that IRS develop a process to identify and evaluate alternative options for improving taxpayer authentication, including technologies in use by industry, states, or other trusted partners; and based on this approach, include and prioritize these options, as appropriate, in its *Roadmap*. IRS agreed with these recommendations, but did not provide additional details on how it plans to address them.

In conclusion, IRS's authentication environment is one component of a broad, complex information technology infrastructure, and we have previously reported on the many challenges the agency faces as it modernizes its tax systems.[7] Taxpayer authentication has become more difficult with the wide availability of personally identifiable information and fraudsters' ability to develop more complex and sophisticated methods to commit fraud undetected. Addressing the issues we describe above could

[7]We have reported extensively on IRS's IT modernization efforts. See, for example, GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems,* GAO-16-468 (Washington, D.C.: May 25, 2016); and *Information Technology: Management Attention Is Needed to Successfully Modernize Tax Processing Systems,* GAO-18-153T (Washington, D.C.: Oct. 4, 2017).

better position IRS to identify and mitigate vulnerabilities in its authentication efforts and better protect taxpayers and the Treasury.

Chairman Jenkins, Ranking Member Lewis, and members of the Subcommittee, this concludes my prepared remarks. I look forward to answering any questions that you may have at this time.

GAO Contacts and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact James R. McTigue, Jr. at (202) 512-9110 or mctiguej@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Key contributors to this testimony include Neil Pinney, Assistant Director; Heather A. Collins, Analyst-in-Charge; Dawn Bidne; and Bryan Sakakeeny.

*Chairman Jenkins. Thank you.

Mr. McKenney, you are recognized.

STATEMENT OF MICHAEL MCKENNEY, DEPUTY INSPECTOR GENERAL FOR AUDIT, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION (TIGTA)

*Mr. McKenney. Thank you. Chairman Jenkins, Ranking Member Lewis, and Members of the Subcommittee, thank you for the opportunity to appear before you today. My testimony today focuses on the IRS's efforts to address electronic authentication on its online applications.

Cyber events against the IRS have illustrated that bad actors are continually seeking new ways to attack and exploit IRS systems to steal taxpayer identities and file 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 gain unauthorized access to tax information in its Get Transcript application.

In March 2017, fraudulent activity caused the IRS to shut down its data retrieval tool on the Department of Education's student aid Web application. In this case, identity thieves were using individuals' personal information obtained outside the tax system to start the student aid application process, and obtain adjusted gross income tax information from the data retrieval tool. The IRS estimated that approximately 100,000 taxpayers were impacted by this data breach.

After the Get Transcript breach was discovered, TIGTA assessed the IRS's efforts to authenticate taxpayers' identities when services are provided to taxpayers. TIGTA made recommendations for the IRS to develop a comprehensive strategy related to its authentication processes. The IRS agreed with these recommendations.

In February 2018, we reported that the IRS had made progress in improving its electronic authentication controls. For example, the IRS deployed a more

rigorous process that provides two-factor authentication via a security code sent to text-enabled mobile phones. However, these improvements were not made to all of its online applications.

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.

In March 2018, we reported concerns about the transcript delivery system, which allows external third-party customers to view and obtain tax information of both individuals and businesses. We found that processes and procedures to authenticate users do not comply with information security standards. For example, the IRS continued to use single-factor authentication, even though its risk assessments in both 2011 and 2015 rated these services as requiring multi-factor authentication to protect taxpayers.

TIGTA is currently evaluating whether the IRS has properly implemented secure electronic authentication controls in accordance with the federal standards for public access to IRS online systems. We anticipate issuing a final report in December 2018.

One challenge that the IRS faces is complying with the new federal security guidelines. Although the IRS has completed risk assessments for its 52 public-facing applications, it has not completed its risk assessments based on the new NIST guidelines issued in 2017. As a result, the IRS cannot say whether its 52 online applications are at their appropriate levels of authentication assurance.

TIGTA has also identified concerns with requests such as the power of attorney declaration of representative form received from individuals seeking to represent taxpayers and access taxpayer information. We found that the process is not sufficient to verify that the actual taxpayer submitted or signed the required form to authorize access to their tax information. TIGTA estimates that the IRS may have processed over 1.1 million unauthorized request forms.

In conclusion, the IRS will continue to face the ongoing challenge of facilitating expanded access to its online tools for millions of taxpayers, while protecting the system from a growing number of sophisticated domestic and international fraudsters. Although improvements in authentication have been made, TIGTA remains concerned about the security of connections to IRS

online systems. 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.

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.

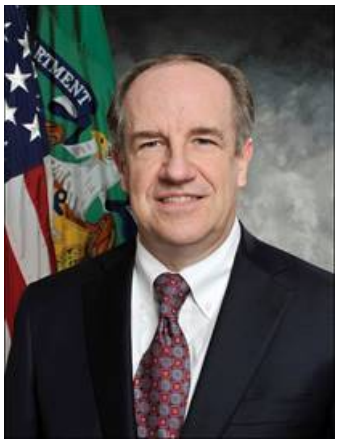
We at TIGTA take seriously our mandate to provide independent oversight of the IRS in its administration of our Nation's tax system. Accordingly, we plan to provide continuing audit coverage of the IRS's efforts to protect the confidentiality of taxpayer data.

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).

*Chairman Jenkins. Thank you. We really appreciate you all being here, we appreciate your testimony, and we are now going to proceed to the question-and-answer session. And I would like to direct my first question to Mr. Killen.

The IRS has said it planned to complete an authentication strategy by the end of 2016. However, in response to GAO's June 2018 report on IRS authentication, the IRS stated that the IRS's "Assurance Strategy and Roadmap" is only a conceptual document.

So what is the current status of the development and implementation of an agency-wide authentication strategy?

*Mr. Killen. Thank you for that question. First, let me say that we appreciate the work done by GAO. We feel it is -- was thoughtful, it was deliberative, and so we appreciate the work done in that study. And, as was mentioned, we have accepted all the recommendations that were delivered to us, pursuant to that, all that.

With respect to our authentication strategy that was developed in 2016, we have actually begun implementation. There are, essentially, 14 initiatives within that strategy, 14 capabilities within that strategy that we are seeking to put in place.

And so, for example, the secure access platform, which is the platform that we have available for taxpayers who need to authenticate, that was -- that is related to the strategy that we have.

In addition, we continue to enhance and focus on monitoring of the performance of that system. We have initiated test-and-learn activities because one of the things that we recognize is that this is a complicated and nuanced space, and so to really continue to, you know, evolve and move the needle forward, it is going to take an all-of-the-above approach. So there will be some things that we will be able to do on our own, some things we will be able to build, some things we will need to engage in strategic partnerships with other federal and private-sector entities.

And so, those are elements within the authentication strategy, and we have initiated test-and-learn pilots in order to sort of prove-out what the marketplace has and what sort of capabilities we can put in place.

So, as an example, we have partnered with a vendor for identity as a service to help augment our ability inside IRS to authenticate taxpayers. We are engaged right now in a call center authentication study. We have assessed all of our level of assurance levels with respect to the former NIST guidance.

Obviously, there is new guidance that has been developed now, but we have engaged in an assessment of that former guidance to try to ensure that, for all of the applications that we have that are customer-facing, that they either meet the guidance as is in place, or they have mitigated and compensated controls in place because taxpayer data protection is something that is extremely important to us. We are 100 percent focused on that day in and day out.

So, although we have work to do on the strategy, because that strategy will be evolving -- because this is not something that stops, you have to continually evolve as the fraudsters and the criminals evolved. You have to adapt with them.

So I do think that we have begun implementation of various aspects of the strategy. We certainly have work to do. And so we agree with that, and we are committed to doing that work because the GAO recommendations were thoughtful, and we will be pursuing each and every one of those recommendations.

*Chairman Jenkins. Do you have a timeline in mind for the development and implementation of this strategy?

*Mr. Killen. Yes, ma'am. The timeline -- and so it really sort of depends on which aspect of the strategy that we are talking about, but sort of -- our next step is to -- as GAO cited, is to do a cost estimation and prioritization. So what that means is -- so the 14 capabilities and initiatives that I had mentioned, our next step with that is to lay out a plan for how we will implement, how we will resource against each and every one of those capabilities within our resource constraints. But that is our actual next step.

But again, that is the next step with respect to prioritizing all of the capabilities and initiatives that we have. But the work that we are doing day in and day out to protect taxpayers, that work goes on unabated, and it has not stopped. But we are looking to lay out the strategy in a sequenced way, so that we will have a longer-term trajectory that we can follow against and that we can resource against, as well.

*Chairman Jenkins. Okay. Mr. McTigue and McKenney, I would like to get your thoughts or views on the IRS's strategy. Can you just briefly tell us what the IRS can do to ensure the successful development and implementation of the strategy?

*Mr. McTigue. Chairman, you know, we liked what we saw in the strategy and road map. It is critical to have a high-level vision and direction. As was pointed out, there -- you know, the strategy was pretty detailed, in terms of having six core objectives, 10 strategic efforts, the 14 initiatives that were mentioned, and 90 activities supporting those initiatives.

What GAO's concern has been is that that is a lot of work, you know, a lot of activities. How much will it cost? You know, what should come first? And, you know, what are the tradeoffs among those activities? And the more information, the more analysis that can support decisions on what to do next and developing the timelines that you are inquiring about, you know, we think that would further strengthen the IRS's approach to improving authentication efforts.

*Chairman Jenkins. Mr. McKenney?

*Mr. McKenney. From our standpoint, we are currently looking at that, and we -- you know, one of the concerns, the main concerns that we have is in terms of making sure that they have a full inventory of those -- all the ways taxpayers can access -- either input information or get information from the IRS, and do a proper risk assessment of those, and, once they do that risk assessment, you know, put those at the proper level of authentication. And that is something we are looking at, you know, right now, and then we will be issuing a report.

But that is -- those are our main areas of focus, to make sure they have a complete understanding of all the ways taxpayers can get in and have that access.

*Chairman Jenkins. Okay, back to Mr. Killen. Does the IRS have plans on how they will measure the progress of the implementation and progress of the strategy?

*Mr. Killen. I think that is -- so do we have concrete measurables that are in place right now, today? I think that the most accurate answer to that is no, because that is not -- we are not quite at that point yet. But I think there are some direct indicators, obviously, that we need to develop.

But I also think this is an area where indirect indicators will be important, as well. And so what I mean by that is -- so, obviously, the world and the space of authentication is very large, it is very broad, because, for us in IRS, what that really comes down to is all of the various transactions that taxpayers conduct with us.

Because essentially, each time a taxpayer is interacting with us to fulfill their tax obligations, for the most part, if they are requesting data, that is data that requires some form of authentication. It is just a matter of what is the level of rigor mapped against the level -- the sensitivity of the data that they are seeking at that particular time.

So there may be one level of rigor associated with, you know, making a payment with us. There may be yet another level of rigor associated with -- if you need a transcript. So my point to that is that assessing measures against each and every one of those transactions is something that is probably not practical. However, I think what we need to do is think about it from the macro standpoint.

So one of the things that we are interested in is, for example, how -- what is the accessibility of IRS taxpayers to be able to access our systems; what are the numbers of taxpayers, who, as they attempt to access our applications that are online, what is the success rate of taxpayers who are able to effectively verify and validate and actually gain access to their information, versus those taxpayers who maybe could not get into our systems because either they didn't possess the information that was needed in order for them to be able to effectively authenticate, or, in the case of more fraudulent activities by criminals, what are the characteristics of that interaction, so that we can use that as an opportunity to further refine our defenses.

So I think my broader point is that we do need to look at what will be the measurables around that. I think we have got good measures with respect to how we are combating fraud, but that is really on the back end. So I think we have work to do with continuing to refine the measures of how our authentication protocol is working holistically, sort of looking at it from end to end.

So I think we have got some work to do in that regard. And again, you know, we are committed to doing that work.

*Chairman Jenkins. Okay. Mr. Killen or Ms. Garza, if you are so inclined, can you -- either one of you -- briefly discuss how the IRS balances providing

the appropriate level of security for its online tool and application while ensuring legitimate taxpayers are able to access those when needed?

*Mr. Killen. So I will give a start with that, and Ms. Garza can jump in.

I think, from my perspective, balance is something that we are -- I don't think that is the right terminology that -- and the right way we want to think about it, because we really want to think about it as a commitment to both. We are absolutely committed to taxpayer security and protecting taxpayers' data, but we are also committed to providing taxpayers with tools and channels in which they can interact with us to fulfill their tax obligations.

So I think what that really means for us is, pursuant to our strategy, we have to ensure that taxpayer information is protected, but we have to also provide for other channels for our taxpayers to interact with us that are rigorous, as well, but that allow them for -- that allow different opportunities for them to interact with us.

So we are really committed to both. And actually, from an authentication perspective, you have to be committed to both because, essentially, if the rigor of your authentication process does not allow the taxpayer to interact with you, that does not mean that we have the luxury to not service them. So we still have to have a way to service those taxpayers that still equally ensures that their data is protected.

So we don't -- we are focused on security day in and day out, but we also have to be focused on providing taxpayers with access because, at the end of the day, they are attempting to fulfill their obligations, and so we have to equip them to be able to do that.

*Ms. Garza. So I would echo what Mr. Killen said. Protecting taxpayer data is paramount. I think we would all agree with that.

But I do believe that we have an obligation to try to provide access to taxpayers. And this is where we are looking at technology to see if there is a way for us to be able to provide the services that people deserve while still maintaining the integrity of our systems and keeping our data secure.

So in -- we are looking at it. We haven't found a silver bullet yet, and -- but we are -- there is a -- I think either GAO or TIGTA mentioned that we had just put out something where you can use your iPhone, IRS2Go, and get an

authentication token that you can use. So we are looking at different technologies that will help people authenticate through our system.

*Chairman Jenkins. Okay, thank you. With that, I would like to recognize our Ranking Member, the Honorable Mr. Lewis, for questions.

*Mr. Lewis. Thank you, Madam Chair. I have a question for each one of you.

How have the recent breaches in both public and private industry impacted the agency's ability to detect and fight identity theft?

*Ms. Garza. I will start with that. Actually, when we heard about all of the different breaches, I was very concerned. I was very concerned with how much data was out there, and how that data could be used against us. And that is actually why we launched the effort about a year-and-a-half ago of reviewing every single transaction that we have with taxpayers of all of our online systems.

So we went through, did a very detailed analysis to identify what data was needed in order to be able to get access, and what kind of authentication procedures or protocols we needed to have in place for all of those applications. So we went through and did that, and basically fortified and secured our online applications.

While we were doing that, the new NIST guidelines came out, and so we actually augmented some of our secure access solutions so that we would be able to be ready for when 63-3 actually came out. Because we started to work on this before it actually came out.

And so it is very concerning that all of that data is out there, and this is where we are continually talking to our stakeholders, with other agencies to come up with ideas and ways to fortify our defenses.

*Mr. Killen. Thank you for that question, Mr. Lewis. I would echo everything that Ms. Garza said, but I would also just say it is very concerning, because the proliferation of personally-identifiable information that is out in the ecosystem makes it fundamentally more difficult to authenticate an individual because, you know, from a simplistic way of stating it, often they have the same information that the legitimate individual has.

So what that means is that we have to be constantly vigilant, and we have to continue to evolve. This is not a static issue, it is an issue that is going to continue to morph and change. And so we have to try to be flexible to change with it, because at the end of the day it comes down to data elements.

What data elements do the fraudsters have who are attempting to impersonate the legitimate individual, and how do we discern who is who? And so what that means is we have to continually, first, be aware of what sort of exposures have been out there, what sort of information do the criminals have access to, and then we have to factor that into how do we adapt our defenses accordingly.

And so we have to be able to change our authentication protocols. And so, you know, that commitment to security and access, that is where the tension comes into play there. Because as those data elements become more and more exposed, we have to make our authentication protocols more rigorous. And if we don't get that dialed exactly right, what ends up happening is legitimate taxpayers can't get through, and they don't have the ability to interact with us.

So we just have to pay constant attention to it. And I think, as Ms. Garza stated, you know, this is one where I think everybody is struggling with this dynamic, where you are in the public or private sector, especially with a customer base our size, 100 or so million taxpayers of all walks of life. So what that means is we are going to have to take an all-of-the-above approach. There will not be one silver bullet.

There will be some things we can do on our own, unilaterally, but in many instances we will need to partner with folks, both in the public sector and in the private sector, as Ms. Garza stated, to help us work through this. And so I think this will have to be a collective effort to get in front of this.

*Mr. Lewis. Care to respond?

*Mr. McTigue. I would just underscore the point that Mr. Killen made and I also made in my statement, in terms of how important it is for IRS to continually evaluate, look at, and test alternatives, evolving technologies and approaches to authenticating taxpayers.

Experts that we have spoken with suggest that maybe a one-size-fits-all approach isn't necessarily the best way. You know, we want to be able to ensure a balance between keeping the fraudsters out, but allowing the legitimate taxpayers in.

And so there may be opportunities to, you know, for example, use the federated model, which would allow credentials established by a tax preparer or a financial institution, or another federal agency such as Social Security or the VA, to be used to access our systems.

Obviously, a lot of work has to be done to ensure, you know, the security of that type of approach. But there are other approaches that could be considered and should be considered as fraudsters become more clever and look for opportunities.

One last point is we have -- you know, the -- we are speaking a lot about online authentication. But, you know, we don't want to overlook the other channels of in-person, telephone, and correspondence, because when data breaches occur -- we have seen a couple examples -- those are the default ways that taxpayers can still receive service. And it is very important to keep monitoring those channels and measure the performance to ensure those are operating effectively, as well.

*Mr. Lewis. I thank you very much.

Madam Chair, will you just yield Mr. McKenney -- let him have an opportunity --

*Chairman Jenkins. Certainly.

*Mr. Lewis. -- to respond? Thank you.

*Mr. McKenney. Sure, thank you. That -- the -- some of the points made are exactly what we would say. And it especially comes into play where they try to implement fraud filters for returns coming in, and that is why they need so many filters, the 200-plus filters that they have. It makes it harder to fine-tune those. They have more false positives, because people can make themselves look a lot like taxpayers.

And once a fraudster has that kind of data, they can -- they constantly try to get more data, by seeing how far they can get through the system. So it becomes highly problematic, in trying to identify who is legitimate and who is not.

*Mr. Lewis. Thank you.

Thank you, Madam Chair.

*Chairman Jenkins. Thank you.

I recognize Mrs. Walorski.

*Mrs. Walorski. Thank you, Madam Chair.

Ms. Garza, I am concerned about our February 2018 report by TIGTA that said the IRS had purchased but not fully implemented network monitoring tools to prevent and detect cyberattacks. What is the current status of the contractor services and technology tools the IRS acquired but, according to the TIGTA report, has not fully implemented? And when do you anticipate they would be fully implemented?

*Ms. Garza. So as of the end of this month, we will be 97 percent complete across all of the online applications. The couple of applications that are still left, we are working through some situations where it may impact the taxpayer. And so we are trying to discuss how to minimize the impact to taxpayers. But I am happy to report that 97 percent of our applications have been -- we have expanded our monitoring tools to just about everything.

*Mrs. Walorski. And you expect that to be fully implemented when?

*Ms. Garza. So, like I said, we are going -- we are talking to some of our business customers to understand how we might -- you know, what we need to do. It is not a question of do we have the technology. Obviously, we have it, it is a question of when do we turn it on and what is the impact to our external stakeholders, once we turn it on.

*Mrs. Walorski. Great, thank you.

Mr. McKenney, TIGTA raised concerns in 2016 regarding the IRS's ability to detect automated cyberattacks. You made seven recommendations to the IRS's Chief Information Officer, including clarifying IRS and contractor responsibilities; monitoring results of controls put in place; and providing adequate tools and training. The IRS agreed with all the recommendations.

Can you give us an update on this? Has IRS implemented all of the recommendations, or are there still areas for improvement?

*Mr. McKenney. I think they are making progress on those recommendations, and we are doing some additional work to evaluate where

they are at on that. But they did agree, and I think they are certainly making progress in that area.

*Mrs. Walorski. It also seems useful that the IRS would fully analyze data captured by its online tools and applications to identify suspicious activity and system weaknesses. However, TIGTA has reported on numerous occasions that the IRS does not analyze its audit logs correctly.

Mr. McKenney, again, can you talk about the concerns TIGTA has about the IRS's lack of adequate review of audit logs, and why is that so important to monitor audit logs?

*Mr. McKenney. The people who commit fraud, if you look at the audit logs, you start seeing patterns of activity, where they are trying to get through the system. If those logs are not formatted in a way that makes them easy to analyze and analyzed consistently and, you know, the criteria needs to be modified so that, you know, they know where the monitoring needs to take place, then those fraudsters, they -- you know, they can go in there undetected.

That is the problem. Once fraudsters, you know, can operate undetected for a while, they can do a lot of damage. So the ability to monitor that activity within the network is really critical.

*Mrs. Walorski. And just one more quick question, Ms. Garza. Why isn't the IRS properly reviewing, analyzing, and distributing its audit logs?

*Ms. Garza. So we have been working very closely with TIGTA on this finding. We have to refine our triggers.

What we found, based on that audit, was that we were doing it on the front end, but we were not doing it on the back end. So we have stood up -- we have now two teams doing -- the cyber analytics team looking through those logs. We have identified -- refined our triggers. We have identified data elements that TIGTA had recommended to us, and have included those.

And right now we are in the process of evaluating the new reports to make sure that they are giving us the kind of results that we are working with. And we really thank TIGTA for their help and support in getting this done.

*Mrs. Walorski. Thank you. Thank you very much. I yield back.

*Chairman Jenkins. Ms. DelBene, you are now recognized for five minutes.

*Ms. DelBene. Thank you, Madam Chair. And thanks to all of you for being with us today.

Mr. Killen, with respect to the IRS's efforts to meet the 2017 NIST standards, you had mentioned that commercially-available solutions that meet these more stringent authentication requirements are not widely available today. Do you have a sense when solutions might be available? And, when they are, what resources, whether it is budget or other resources it might take to accommodate those?

*Mr. Killen. I think this might be another one where maybe we can sort of tag-team the answer.

*Ms. DelBene. That is fine.

*Mr. Killen. But I will just say that I think, you know, this is another aspect where the considerations are sort of nuanced also, because when you look at the new standards and those of the NIST 863 standards that were released last year, identity-proofing has been separated from authentication.

And so, when you talk in terms of identity-proofing, it really is a product of what evidence are you collecting, and then who has the ability to actually validate the authenticity of that data collected. So whether it be driver's license or passports, or some other sort of information, who has -- what technology, what entity has the ability to validate the authenticity of that data. And then, secondly, to match that data that has been authenticated back to the individual who is trying to conduct business with us.

So what that means from a technological availability standpoint, I won't say that there is not technology available. I think one of the considerations -- and there are many -- is is it available at scale for the number of customers that we have, and is it available with sufficient redundancy, so that you are not tied or locked into one technology, one vendor, one solution that would put you in a place of concern, if something happened with that technology or solution.

I will defer to Ms. Garza.

*Ms. Garza. So let me add a couple of things. One, to the last point that Mr. Killen was talking about, there is also a question about certification. Who certifies that this publicly-available product actually meets the standard?

And so there is some conversations that we are having with GSA and with SSA and with the Treasury Department about what that process is going to look like, so that -- we don't want to just go out and get any solution, we want to get a solution that is actually certified that it is going to work against the new NIST standards.

Having said that, overall, what -- like Mr. Killen said, they have separated the ID-proofing component with the authentication component. Our solution today meets the authentication component of the new NIST standards.

They also -- we also have implemented -- there is a whole new risk assessment approach that we needed to make sure that we did to evaluate it against the new standards. We have completed that work. We have piloted that work. And we anticipate we will evaluate every single one of our online applications before -- in a year's time.

In the meantime, we will be working to determine -- we are working with SSA and GSA and others to try to find a solution that would meet the requirement around the ID-proofing component.

*Ms. DelBene. Okay, thank you.

Ms. McTigue, the IRS -- we have been talking about their efforts to meet the 2017 NIST guidance. But that guidance still applies to the entire Federal Government. And so I wondered. What is your view of how other agencies are handling this? And is the IRS kind of on track with others? Is there a difference, or best practices that you can talk about?

*Mr. McTigue. Actually, Madam Congressman, we have work underway looking at a few select agencies across the government to see what they are doing, the progress they are making, and, you know, the steps that they are following to implement the 2017 guidance.

We hope to have a report out, I think, early spring, maybe the February timeframe. So we are looking at it, and it is a little bit too early to say.

*Ms. DelBene. But that would give us a sense of how some folks are -- maybe found some solutions that could be shared in other agencies, and how to use those --

*Mr. McTigue. Oh, absolutely.

*Ms. DelBene. Okay.

*Mr. McTigue. Absolutely.

*Ms. DelBene. Thank you very much. I yield back.

*Chairman Jenkins. Thank you.

Dr. Wenstrup, you are recognized for five minutes.

*Mr. Wenstrup. Thank you, and thank you all for being here. I am not sure who can answer this question – I'll ask for anybody.

But certainly, we are not the only industrialized country that collects taxes and that probably has -- we are probably not the only country that has been subject to fraud and security challenges. So I am just wondering how we compare to other nations, and are we looking at that to find best practices to prevent fraud and increase security.

*Ms. Garza. So I will take that. Actually, we have met with other countries. In particular, with Europe, England, United Kingdom -- sorry, lost that for a while. And we actually brought the individual in who had expertise in this area to advise, actually, my entire team on the techniques that they are using in order to combat -- because, you are right, they have the same issues that we have. And so we took some pointers from him as to what the solution is.

They are using different kinds of techniques. A lot of it has to do with -- they are using -- like France is using tokens of some kind. They are using -- they were looking at facial recognition as another possibility.

And so we have had some conversations with other countries, but the ID proofing part is the hard part of this. Everyone is solving for the authentication piece, but the ability to ensure that the person that you are talking -- the taxpayer is who they say they are, that is the part where people seem to be having a hard time finding. And that is why we are having a hard time finding a solution for the ID-proofing part.

*Mr. Wenstrup. Yes, I think there may be some real value in entertaining conversations with other governments' agencies, because a lot of this fraud is not domestic, you know, it is coming out of Nigeria and everywhere else, right? So I don't think they really care if they steal dollars or pounds.

And so we may be able to share information in ways that we can stop some of these things in their tracks, if we are collaborating on finding where it is coming from, and how they are doing it. So I may suggest we do more of that, and also come up with best practices. But see, we have got common enemies in this regard.

*Ms. Garza. Yes. We did have a study. We asked one of our vendors to look at other countries, and they provided us with a kind of a high-level summary. But we will continue to do that.

*Mr. Wenstrup. Mr. McTigue?

*Mr. McTigue. Congressman, I would underscore I think that is a -- you know, a very important place to look. But I would also reiterate what IRS is doing with the Security Summit. You know, some of our states are bigger than -- you know, have bigger economies than many other countries. And so, you know, I think the Security Summit is a mechanism that is working well and has the potential to generate additional results.

In the work that we did, in our June 2018 report, you know, we did go out to some states. Other countries were outside the scope, but states are facing similar problems. They are looking at different technologies, some utilizing driver's license information, pictures. Gina mentioned facial recognition technology.

So, I mean, there are ideas out there. And again, this underscores the importance of looking broadly and continuously at developing technologies and approaches.

*Mr. Wenstrup. I appreciate that approach.

Yes, Mr. Killen?

*Mr. Killen. I will echo both of those comments. You know, this is an area where no one has a monopoly on the best ideas. And so we are open for great ideas wherever they come from.

The Security Summit, I would be remiss if I didn't mention that, because that, in many ways, I think, has been transformative for us, because, you know, protecting taxpayers is in the interest of everyone within the tax ecosystem.

And so, you know, we realized several years ago that this was a job that was too big for everyone to continue to operate in their individual silos, whether it was IRS, or whether it was state departments of revenue, or the private-sector tax industry.

And so, as an example, one of the aspects that I think we have made some tremendous progress on -- really, two. The first is we have an authentication working group within the Security Summit. So one of the things they have been working on are what we would call trusted customer requirements, because, you know, to the extent that you can stop this problem on the front end, it protects taxpayers on the back end so you don't have folks burdened.

And then we have a group that has been focused on working with the states and the industry to all align on common security standards and share emerging threats and trends from a cybersecurity perspective, so everyone can harden their defenses.

*Chairman Jenkins. Thank you.

*Mr. Wenstrup. Thank you, I appreciate that.

*Chairman Jenkins. Mr. Bishop, you are recognized for five minutes.

*Mr. Bishop. Thank you, Madam Chairwoman, and thank you to the panel today. I appreciate your being here today.

In Mr. McKenney's prepared statement I noticed that there was a rather alarming statistic that the IRS has 52 forward-facing applications. And I get the idea of access to taxpayers, I think that is a great idea. But it seems to me that, as we discuss privacy and record management and cybersecurity of all the taxpayer data, it seems to me that many forward-facing portals is a disaster waiting to happen.

And I am just wondering what the purpose of the 52 forward-facing applications are, and if in fact that is an issue for the IRS, and if there is a concern that maybe we want to -- a more focused approach to the way in which we provide access to data for taxpayers.

*Mr. Killen. Well, I can start and let Ms. Garza or others, even, come in.

So we have 100 to 120 million taxpayers, all with needs to conduct business and transactions with the IRS, whether it be for individual taxpayers, or

whether it be small businesses, whether it be representatives who are authorized to do business on behalf of their taxpayers. And so I won't say that I have a true understanding of what each and every one of those applications do.

I think, you know, your question is an insightful one. I would just say that I think each application that we have is there because some taxpayer somewhere, some group of taxpayers find great value in it. But I think, you know, obviously, it is important for us to always assess whether there is a true business need for applications and services that we provide. Application, essentially, is a service to a taxpayer in some way, shape, or form, whether it is for a taxpayer to get a transcript, to make a payment with us, to check their account.

So I would just say -- so I appreciate the essence of the point, and that is you have so many taxpayer public-facing, you know, applications that, you know, there could be a perspective that that could increase the risk. I think the challenge there is inherently we are a public-facing organization because taxpayers have to adhere to their tax requirements, and so we work to try to make it as easy for them to be compliant with their tax obligations as we can.

But we will --

*Mr. Bishop. Thank you. Thank you.

Ms. Garza?

*Ms. Garza. The only thing that I would add to that -- so there are 52 online transactions where we exchange information with the taxpayer. Part of our strategy is to move all of those applications that we can behind our secure access solution. And for our highest-risk applications, we have done that. So the ones that were at the highest risk, might have been providing more PII information, those have been moved behind that.

But then there are other kinds of applications like Make a Payment. Most fraudsters are not going to go and try to make a payment to the IRS.

So I think there is a -- I understand the concern. I think what we have done is that we have consolidated the protection layer that we are using, and put our most sensitive applications behind that layer.

*Mr. Bishop. Okay. Thank you very much for that.

*Mr. McTigue. I would just like to add that we currently have work undergoing looking at the suite of online services that IRS offers and, you know, whether or not that makes sense. So hopefully we will answer some of your questions.

*Mr. Bishop. That is a huge question, and we have a limited amount of time. I am sorry that I didn't -- we don't have more time to talk about it, but I would like -- if you want to talk more about it, I would love to hear about it.

Dr. Wenstrup mentioned today that he thinks that you should review what other countries are doing. I think that is a great idea. I also think that when it comes to developing this -- and implementing online multi-factor authentication, that the idea of getting the private sector involved is a really important process. And I am very glad to hear that the Summit has produced that kind of working relationship. I hope that continues.

One other concern I had, it is very -- we are running out of time -- is to ask Mr. McKenney -- the taxpayers can grant power of attorney to get information, and you have raised some concerns in your written testimony that there may not be protections in place for these forms that are used. And I wondered if you might be able to comment on that really quickly.

*Mr. McKenney. Right. And that came as a result of the IRS evaluating that, and taxpayers being completely unaware that they had a representative authorized to look at their account. And when you project it out, it is pretty serious. It is over 1.1 million, when you project how many people this might affect.

The mitigating control, which is some benefit, is going to send a notification to the taxpayer to confirm that they have authorized that. So I think that is a mitigating control for the -- until they can put some online process in place.

*Chairman Jenkins. Thank you.

*Mr. Bishop. Thank you, Madam Chairman.

*Chairman Jenkins. Mr. Curbelo, you are recognized for five minutes.

*Mr. Curbelo. Madam Chairman, thank you for this hearing, and I am grateful to all the witnesses. For me and for my community in South Florida, this is an issue of major concern. Sadly, South Florida is known for seeing a disproportionate share of fraudulent activity, whether it be tax fraud, Medicare

fraud, insurance fraud. And it is something that our community wants to fight, and our community wants to see progress on all these fronts because, of course, when people defraud the government, they are defrauding the public, fellow taxpayers. So I am grateful for this opportunity.

And a lot of my questions have been answered in previous exchanges. But I think all of us agree that technology is probably the cure to a lot of these challenges that we face.

So I just wanted to ask, broadly, if the agency is at all looking forward at technologies such as blockchain that, in the future, could make all of these transactions a lot safer, in the view of many, at least for now, completely secure, with zero risk. Is that something that is on the agency's radar? I will let anyone answer.

*Ms. Garza. So yes. We have been looking at blockchain. We have met, actually, with several vendors with that offering. We have explored the possibilities.

Here again, it is not a complete solution. The part that most of these solutions keeps missing is the -- making sure -- before you set up the blockchain, that kind of security control, you have to already have known that the person is who they say they are. That is the part that has been very hard to solve.

Blockchain will work, it is -- you are correct, it is very good. But if you are block-chaining the wrong person, then it didn't help. So that is what we are trying to work through, and that is where we are trying to explore for new solutions around the ID-proofing component.

*Mr. Curbelo. Thank you.

Does anyone else have anything they want to add?

Well, thank you, Madam Chairman. I appreciate it. I yield back.

*Chairman Jenkins. Thank you and, again, thank you to all of our witnesses for being here today.

Be advised that Members have two weeks to submit written questions to be answered later in writing. Those questions and your answers will be made part of the formal hearing record.

And with that, the Subcommittee stands adjourned.

Thank you.

[Whereupon, at 11:45 a.m., the Subcommittee was adjourned.]

MEMBER QUESTIONS FOR THE RECORD

HOUSE COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON OVERSIGHT
QUESTIONS FOR THE RECORD FOR
MICHAEL MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
SUBMITTED BY REPRESENTATIVE DARIN LAHOOD

September 26, 2018

"**IRS Taxpayer Authentication: Strengthening Security While Ensuring Access**"

1. In your testimony you mentioned that 26 of the IRS's online tools and applications were not at their assessed level of assurance. How concerned is TIGTA about that and what is IRS doing to ensure that it will not face an increased and unnecessary level of online security risk when authenticating users?

   Answer: The level of risk varies among these 26 online applications based on the type of information that can be requested or accessed. As such, TIGTA still has moderate concern over some of the applications that were not at their assessed level of assurance. Furthermore, the IRS's still needs to evaluate all online applications based on the new National Institute of Standards and Technology (NIST) standards[1] adopted in June 2017. The OMB expects Federal agencies to meet NIST requirements within one year of publication, and the IRS is in the early stages of this effort.

   At the time of our audit, the IRS was in the process of creating the Identity and Access Management office in the Applications Development organization to provide direction for all application development activities for external identity proofing, authentication, and authorization. This office will work across the Information Technology organization and with other business operating divisions to identify digital identity and authentication needs throughout the IRS by:

   - *Ensuring adherence to Federal security standards, such as those of the NIST.*
   - *Supporting the development and delivery of new and existing public-facing applications.*
   - *Collaborating across Federal agencies to implement Federal security initiatives.*
   - *Coordinating and collaborating on cybersecurity, internal identity, and access management activities with stakeholders.*

   TIGTA plans to continue conducting audit work in this important area. As we have learned from recent data breaches, the IRS must remain vigilant in monitoring and improving the authentication approaches for all applications because criminals are constantly seeking new ways to steal taxpayer and personally identifiable information.

[1] NIST SP 800-63-3, *Digital Identity Guidelines* (June 2017).

QUESTIONS FOR THE RECORD
COMMITTEE ON WAYS AND MEANS
OVERSIGHT SUBCOMMITTEE
"IRS TAXPAYER AUTHENTICATION: STRENGHTENING SECURITY WHILE ENSURING ACCESS"
SEPTEMBER 26, 2018

Questions from Chairman Jenkins

1. **During your testimony, you described that in 2015 the IRS established the Identity Assurance Office to help the IRS better understand authentication and fraud detection needs across the agency. The Treasury Inspector General for Tax Administration (TIGTA) and Government Accountability Office (GAO) as a part of their work on the IRS's authentication efforts have discussed a number of parties inside the IRS that provide input to aspects of the IRS' s authentication efforts. Please list (1) all entities within the IRS that are involved in decision-making and directing policy where online authentication is concerned, (2) how the various entities involved coordinate their activities within the IRS, and (3) the entity that ultimately is responsible for ensuring the success of the IRS's online authentication efforts.**

IRS Response to Question 1: The success of the IRS's online authentication efforts is a shared responsibility across many functions. The IRS has structured governance with respect to the online authentication by establishing the Authentication, Authorization, and Access (A3) Executive Governance Board (EGB). The A3 EGB governs selected investments and their systems, programs and projects, as delegated by the Services and Enforcement (S&E) Executive Steering Committee (ESC) and, as appropriate, the Information Technology (IT) Strategic Development (SD) ESC. Through this governance role, the A3 EGB supports Service-wide A3-related strategy execution by building and operating more consistent approaches for the A3 needs across IRS functions and programs. The A3 EGB provides concurrence, guidance, and information sharing on A3 priorities, risks, strategic direction, and resource management. Policy guidance for the IRS's online authentication efforts resides with the S&E ESC.

2. **During the hearing, you described that the IRS has put its most sensitive tools and applications behind Secure Access. Please discuss (1) how many individuals have successfully passed Secure Access' s multifactor authentication, (2) what was the Secure Access pass rate for individuals attempting to authenticate their identities in 2017 and 2018, and (3) how many tools and applications does the IRS plan to add to Secure Access in 2019.**

a. **Does the IRS currently have a goal for the percentage of taxpayers it would like to have success fully verify their identities through Secure Access?**
b. **What other metrics does the IRS use to evaluate the accessibility of its online tools and applications?**
c. **What options are available to legitimate taxpayers who fail the Secure Access authentication process but would still like to access the IRS' s online tools and applications behind Secure Access?**
d. **The IRS' s Electronic Tax Administration Advisory Committee recommended in June 2018 that the IRS investigate the use of trusted third parties as an alternative to conduct in-person identity proofing to enable taxpayers to ultimately gain remote secure access to their information. To what extent does the IRS use or plan to use third parties for authentication services?**
e. **Does IRS currently have any plans under way to develop other mobile applications, similar to IRS2GO? If so, please discuss those mobile applications.**
f. **To what extent does the IRS have plans to develop and implement an online third- party authorization tool that would supplement the processing of paper copies of IRS Forms 2848, Power of Attorney and Declaration of Representative and Form 8821, Taxpayer Information Authorization?**

IRS Response to Question 2(1): Secure Access's multifactor authentication has had 6.5 million taxpayers register as of September 30, 2018.

IRS Response to Question 2(2): The Secure Access multifactor authentication verification rate for fiscal year 2017 was 33.3% and for fiscal year 2018 it was 39.2%.[1]

IRS Response to Question 2(3): The IRS currently has no plans to add additional applications to Secure Access in fiscal year 2019, with the possible exception of a tax professional account as described in response 2(f) and pending further solution design activities. The IRS has an online account for individual taxpayers and increases the functionality of that system using its agile development program which allows the IRS to identify projects and then develop new functionality on a nine-week cycle. While this is not a new FY 2019 application, the IRS is following the best practices of industry and continuously improving the service provided to taxpayers by means of this existing online application. Additionally, the IRS plans to continue increasing security for select online applications protected by Secure Access during FY 2019.

IRS Response to Question 2(a): Our goal is to continuously improve the user experience and increase coverage while protecting taxpayer data and the security of the system. The percentage of taxpayers who successfully verify their identities through Secure Access is one of several indicators of both the security and usability of our taxpayer services.

IRS Response to Question 2(b): As part of the Authentication Strategy, the IRS has committed resources to systematically analyze the Secure Access user experience and use data analytics results to improve screen wording, user input fields, and error messaging. This analysis includes assessing the user experience by application, volume and user type (e.g. new, returning).

IRS Response to Question 2 (c): While taxpayers may always access their information using traditional customer-service channels (i.e., phone, in-person, by mail), some taxpayers who are unable to authenticate through Secure Access may be able to finish the process by mail and thereafter establish an online profile and use that profile to access their information online. Taxpayers who fail the initial IRS identity verification steps or the financial verification steps may only obtain services through other channels. In contrast, customers who satisfy the identify and financial verifications steps but who cannot register successfully because they do not have a phone or they failed the phone verification step may request an activation code by mail (sent to their mailing address of record) and may use that code to establish their online profile and thereafter use their profile to access their information online.

IRS Response to Question 2(d): The IRS appreciates this recommendation, which aims to help improve service to taxpayers. The IRS will develop requirements in accordance with the NIST SP 800-63C, *Digital Identity Guidelines: Federation and Assertions*, by the end of fiscal year 2019. Once the requirements are developed, the IRS will examine the feasibility of a short duration, limited scope innovation study to evaluate these requirements.

IRS Response to Question 2(e): IRS2Go is the official mobile app of the IRS and currently provides a platform for several online capabilities for taxpayers such as checking refund status, making a payment, finding free tax preparation assistance, signing up for helpful tax tips, and generating login security codes for certain IRS online services protected by Secure Access. Future mobile service options may be added based on taxpayer needs and other factors.

IRS Response to Question 2(f): The IRS is in the process of creating detailed requirements for a tax professional account. This concept has been vetted with tax professionals at IRS National Tax Forums and other venues. Delivery of the tax professional account feature is expected to require a high level of effort, and to mitigate

risk, the IRS will build and roll out these features in an incremental and iterative development process, similar to how the IRS implemented individual taxpayer online account -- incrementally and growing in capabilities over time. Future capabilities common to both the tax professional account and the taxpayer account will include digital equivalents of Form 2848 or 8821 used to establish representational or information access rights. Given the range of tax professionals and taxpayers that the IRS interacts with each day, it is expected that the IRS will continue to receive and process paper Forms 2848 and 8821 even after the IRS has developed and launched the tax professional account.

3. **During the hearing, you discussed that the IRS is currently not compliant with the new National Institute of Standards and Technology (NIST) digital identity guidelines (SP 800-63-3), in particular the identity proofing component but the IRS has completed risk assessments.**

    a. **Does the IRS expect to fully comply with the 2017 NIST digital identity guidelines by the end of the 2019 filing season? If not, when does the IRS expect to fully comply with the new NIST digital identity guidelines?**

    b. **How many of the IRS's 52 tools and applications are currently operating below their assessed Identity Assurance Level (IAL) and Authenticator Assurance Level AAL)? Are any of those tools and applications with an IAL and/or an AAL of two or greater currently not behind Secure Access?**

    c. **What additional oversight or monitoring of the IRS' s online tools and applications does the IRS complete where there is a discrepancy between the assessed and implemented IAL and AAL?**

    d. **What mechanisms does the IRS have in place to coordinate with other agencies on their compliance with the NIST digital identity guidelines?**

IRS Response to Question 3: The IRS is committed to continuously improving our authentication procedures in line with guidelines from the Office of Management and Budget (OMB) and NIST, which apply to all federal agencies implementing digital identity services.

When NIST revised its guidelines in June 2017 with the release of NIST SP 800-63-3, it was a complete rewrite of the eAuthentication standard that created a new framework

for federal agencies to improve the security of their identity-proofing and authentication programs. The new guidelines introduced new concepts and redefined how federal agencies implement digital identity services. Further, the new standard has substantially more rigorous requirements than the previous standard.

The IRS is working to assess how the new guidelines affect the processes and systems that taxpayers use, and we have taken preliminary steps to implement the guidelines. For example, we developed a comprehensive, data-driven approach to assess applications against the new NIST guidelines and have begun testing the new process.

One of the first steps we took was to determine the extent to which existing applications might meet the new NIST standards. For example, we assessed the Secure Access system against the new NIST guidelines and we found the IRS meets Authentication Assurance Level (AAL) 2 and Identity Assurance Level (IAL) 1 requirements. However, like all federal agencies, the IRS faces challenges implementing the new NIST standards across all of our applications.

As we progress on implementing these new standards, we continue to safeguard taxpayer information through the implementation of strong mitigations and compensating controls to strengthen the overall security of online services. An example is enhancements to network monitoring controls to help block suspicious activity on IRS.gov and thus thwart cybercriminals' attempts to obtain unauthorized access to taxpayer data through our online applications.

We emphasize that the cyber landscape is consistently shifting, requiring stronger identity proofing and authentication requirements and robust cyber monitoring tools.

IRS Response to Question 3(a): The IRS is working to assess how the new guidelines affect the processes and systems that taxpayers use, and we have taken preliminary steps to implement the guidelines. We currently do not have an expected completion date, but work in this area is underway.

IRS Response to Question 3(b): Over the last several years, we have focused on strengthening our online identity proofing and authentication processes, and we have made significant progress. In our initial review, we believe many of our transactions will be assessed at AAL2 and we are fully compliant with AAL2. We anticipate completing comprehensive assessments on all externally-facing transactions by the fall of 2019. These assessments will help inform the extent to which IRS tools and applications have the proper identity proofing and authentication procedures in place. In parallel, we have partnered with the Department of the Treasury and the Social Security Administration to identify an "identity proofing solution" that meets the IAL level 1 and level 2 standards.

IRS Response to Question 3(c): Where necessary the IRS implements strong mitigations and compensating controls to strengthen the overall security of online transactions. These include additional technical and management controls, as well as other reasonable mitigations to safeguard taxpayer information. For example, with implementation of network monitoring capabilities, we now have the ability to get automated alerts based on anomalies detected.

IRS Response to Question 3(d): The IRS actively participates in recurring meetings and forums with the Treasury Department, Treasury Bureaus, the Social Security Administration, the NIST, the General Services Administration (GSA) and other stakeholders in this arena.

Questions from Rep. LaHood

4. **For those online tools and applications where there is currently a discrepancy between the assessed IAL / AAL and implemented IAL / AAL, has the IRS developed plans to bring those tools and applications into alignment?**

IRS Response to Question 4: The IRS is assessing how the new guidelines affect the processes and systems that taxpayers use, and we are taking preliminary steps to implement the guidelines. Our goal is to ensure we use adequate security controls and where necessary, we implement strong mitigations and compensating controls to strengthen the overall security of online services. We do not currently have an expected completion date for bringing all tools and applications into alignment with the new NIST guidelines, but work in this area is underway.

5. **When does the IRS expect full compliance between the assessed IAL/ AAL and implemented IAL/ AAL for all of its 52 online tools and applications?**

IRS Response to Question 5: The IRS is working to assess how the new guidelines affect the processes and systems that taxpayers use, and we have taken preliminary steps to implement the guidelines. We currently do not have an expected completion date for bringing all tools and applications into compliance with the new NIST guidelines, but work in this area is underway.

[1] Represents activity since the December 10, 2017 relaunch, (after the October – December 2017 temporary shut-down).

PUBLIC SUBMISSIONS FOR THE RECORD

American Association of
Motor Vehicle Administrators

safe drivers
safe vehicles
secure identities
saving lives!

September 24, 2018

United States House of Representatives
Ways and Means Committee
1102 Longworth HOB
Washington, DC 20515

RE: The Internal Revenue Service's Taxpayer Online Authentication Efforts

Chairman Brady, Ranking Member Neal and Members of the House Ways and Means Committee:

On behalf of the American Association of Motor Vehicle Administrators (AAMVA) and its state-based membership, thank you for holding this important hearing on the Internal Revenue Service's Taxpayer Online Authentication Efforts. AAMVA respectfully requests that this statement be made a part of the official record of this hearing.

We would like the Ways and Means Committee to consider the sustained efforts state departments of motor vehicles have made in vetting and protecting their constituents' identity, and to consider a tool known as the Driver's License Data Verification (DLDV) service in particular. Given that motor vehicle administrators have long understood the dilemma of applying complex public safety data to a single evolving record (among millions), AAMVA members understand the challenges associated with verifying people "are who they say they are." Realizing that the use of fraudulent identity and the proliferation of cybercrimes and technology exposes a wider sector of government services beyond the public safety sector, AAMVA and its membership developed the DLDV service. DLDV provides government entities with the real-time capability to verify Driver License and Identification Card credentials with data from the issuing jurisdiction. This capability reduces the ability of criminals to use a counterfeit or assumed credential that does not carry the exact data attributes assigned to it by an issuing jurisdiction. Further, it ensures that the data associated with a credential *continues* to align with the data of the issuing authority beyond the point of issuance.

The DLDV system has been used to effect and is a tool that could also be used by the IRS to strengthen its taxpayer authentication efforts.

The Social Security Administration (SSA) leveraged this tool when looking for a way to enhance its ability to verify applicants for an on-line replacement social security card. Realizing that individuals may present counterfeit or fraudulent credentials to access the online SSA service, the SSA approached AAMVA on a solution to mitigate this risk. DLDV became that solution, closing the loop on an individual's ability to use a credential that was not officially issued by a driver's license agency. Now, when an individual requests a replacement card through SSA's internet-based Social Security Number Replacement Card program (iSSNRC), SSA runs a DLDV

check of the attributes on the person's state-issued identification credential. To date, 35 states are employing DLDV in conjunction with SSA to replace their Social Security cards online. In addition, the Unites States General Services Administration is utilizing DLDV to verify an individual's identity as part of login.gov, which assigns online access privileges to federal services and websites for each identity record.

In real-time, DLDV compares the data fields provided by GSA or SSA from the individual's identity credential against the data of record at the respective motor vehicle agency. AAMVA returns a true or false indicator to GSA or SSA for each data field submitted for verification. No personally identifiable data is stored by AAMVA, as AAMVA deletes both the SSA, GSA and motor vehicle agency data immediately after providing the match results. AAMVA invites the Committee to review its work with respect to DLDV at https://www.aamva.org/DLDV/.

Thank you for your consideration. Please feel free to contact me or Cian Cashin if you have any questions. Cian and I can be reached at ccashin@aamva.org or aferro@aamva.org, respectively.

Sincerely,

Anne S. Ferro
President & CEO

ASF/sfb

Founded in 1933, AAMVA is a tax-exempt, nonprofit organization developing model programs in motor vehicle administration, law enforcement and highway safety. AAMVA represents the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws and serves as a liaison with other levels of government and the private sector. Its development and research activities provide guidelines for more effective public service.

Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

CDIAONLINE.ORG

October 1, 2018

The Honorable Lynn Jenkins, Chairman
The Honorable John Lewis, Ranking Member
Committee on Ways & Means, Subcommittee on Oversight
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Jenkins and Ranking Member Lewis:

Thank you for holding the hearing entitled, "IRS Taxpayer Authentication: Strengthening Security While Ensuring Access" on September 26, 2018. We share the Subcommittee's commitment to ensuring IRS taxpayer authentication procedures are secure, accessible and equipped to operate efficiently in today's dynamic business environment.

The Consumer Data Industry Association (CDIA) represents, among others, companies that belong to the IRS' Income Verification Express Services (IVES) Participants Working Group. Collectively, as participants in the IVES program, these companies serve lenders across the country by processing 4506-T forms through the IRS to verify important financial information submitted by prospective borrowers. Independently, they each secure their data through enterprise-level systems supported by data security experts and industry-leading protocols.

With sophisticated cybersecurity and privacy threats in the market, our member companies have made protecting sensitive taxpayer information a top industry priority by taking proactive steps to work with the IRS to craft effective systemic solutions.

In December 2017, our companies were notified by the IRS that new multi-factor authentication protocols known as Secure Access would be enacted within the broader e-Services platform as part of ongoing efforts to secure sensitive taxpayer information. In response, IVES participants worked tirelessly to prepare their internal systems to comply with the new authentication process. Concurrently, we engaged in direct communication with IRS leadership to work through technical issues and ensure timely retrieval of tax transcripts to allow the downstream mortgage lending process to continue uninterrupted.

Following the implementation of Secure Access, in January 2018 the IVES Participants Working Group was created by the IRS at the request of mortgage lenders, servicers and vendors. Since its inception, the Working Group has met quarterly to discuss ways to improve the IVES system from a security and operational standpoint with the overarching goal of working towards the creation of a modern, secure and fully integrated Business to

Government (B2G) solution as articulated in HR 3860, the IRS Data Verification Modernization Act of 2017.

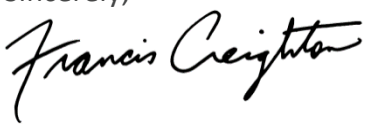
The latest taxpayer authentication and data security issue being discussed between our companies and the IRS through the Working Group is the ongoing planned redaction of Personally Identifiable Information (PII) from the transcript responses the IRS provides our companies from 4506-T requests. Although we agree that certain PII redaction is important, in May 2018 the IRS agreed to push the implementation date for PII redaction from August 2018 to January 2019 to allow our technical teams adequate time to properly design, build, test and implement the necessary changes required to our existing operating systems. These changes include creating an effective Customer File Number (CFN) coding system for matching transcripts in the absence of PII such as full taxpayer names, Social Security Numbers and addresses. Over the next quarter, we will continue to prepare for PII redaction implementation in January 2019.

We share the Subcommittee's commitment to protecting taxpayer information through secure and accessible taxpayer authentication procedures. We believe that the IRS' decision to implement Secure Access in the form of multifactor authentication and ongoing efforts to redact certain PII are strong steps to help protect the American taxpayer. As the Subcommittee continues to evaluate existing taxpayer authentication procedures and process improvements, we encourage the serious consideration of ways to support the creation of a secure and fully integrated B2G solution that can operate in today's dynamic economy and protect against evolving threats.

As an industry, we support efforts by Congress to invest in the IRS' information technology system and are encouraged by the dialogue taking place with IRS leadership on the best ways to update critical systems in the future. We maintain that creating a fully integrated, internet-based B2G solution for taxpayer authentication would be in line with long held industry views that modern system-wide updates would be more beneficial for data security and business operations than a piecemeal approach.

We thank the Subcommittee for the chance to comment on ongoing taxpayer authentication procedures and would welcome the opportunity to meet with the Subcommittee to discuss ways we can work together to achieve our common goals around this critical issue.

Sincerely,



Francis Creighton
President & CEO

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

September 26, 2018

The Honorable Lynn Jenkins
Chairman
U.S. House Committee on Ways and Means,
Subcommittee on Oversight
1102 Longworth House Office Building
Washington, DC 20515

The Honorable John Lewis
Ranking Member
U.S. House Committee on Ways and Means,
Subcommittee on Oversight
1102 Longworth House Office Building
Washington, DC 20515

Dear Chairman Jenkins and Ranking Member Lewis:

The Electronic Privacy Information Center (EPIC) writes to you today to ensure that the Internal Revenue Service (IRS) takes adequate steps to protect taxpayers' most sensitive information from inadvertent disclosure or theft.[1] EPIC has testified in Congress about the need to increase privacy safeguards to prevent the misuse and theft of Social Security Numbers (SSN) and other identifying information,[2] and maintains an extensive archive online about potential harms stemming from misuse or wrongful disclosure of SSNs.[3]

Nearly seventeen percent of all identity-theft complaints to the Federal Trade Commission in 2017 stemmed from instances of tax fraud.[4] The IRS contributed considerably to this number: identity thieves using the online IRS Data Retrieval Tool stole the personal information of up to

[1] *Hearing on the Internal Revenue Service's Taxpayer Online Authentication Efforts*, U.S. House Comm. on Ways and Means (Sept. 26, 2018), https://waysandmeans.house.gov/event/hearing-on-the-internal-revenue-services-taxpayer-online-authentication-efforts.
[2] *Hearing on Securing Americans' Identities: The Future of the Social Security Number Before the Subcomm. on Soc. Sec. of the H. Comm. on Ways and Means*, 115th Cong. (2018) (statement of EPIC Consumer Privacy Fellow Sam Lester), https://epic.org/testimony/congress/EPIC-Testimony-HW&M-SS-Subcomm-5-17-18.pdf; Statement of EPIC to Reps. Johnson, Larson, Hurd, and Kelly (May 22, 2017), https://epic.org/testimony/congress/EPIC-HCOGR-SSN-May2017.pdf.
[3] EPIC, *Social Security Numbers*, https://epic.org/privacy/ssn.
[4] Fed. Trade Comm'n, *Consumer Sentinel Network Data Book 2017: Identity Theft Reports by Type* (2018), https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/consumer-sentinel-network-data-book-2017/id-theft-reports-by-type.

100,000 taxpayers.[5] This IRS tool was deployed on federal student-loan websites,[6] leaving students exposed to this fraud. The IRS estimated that this lapse ultimately cost over $30 million in fraudulent tax returns.[7] EPIC has repeatedly highlighted the unique risks students face to their privacy,[8] and we encourage the Subcommittee to investigate this immense data breach.

The inability of the IRS to protect sensitive taxpayer information is pervasive throughout the agency. Besides allowing thousands of taxpayer records to improperly become public, the IRS repeatedly left identified network vulnerabilities unpatched,[9] failed to encrypt transfers of sensitive taxpayer data to third parties,[10] and did not follow its own data security and privacy procedures.[11] The IRS Inspector General recently concluded that "IRS policies are not in compliance with Federal electronic records requirements."[12]

This cannot continue to be the state of affairs. As the Subcommittee examines IRS record-keeping practices, it must ensure that the IRS provides sufficient oversight of its employees and contractors—especially those in possession of sensitive taxpayer information. The Subcommittee should ask the IRS why it has not addressed these, and other identified issues, and should also press the IRS to ensure that online authentication systems are routinely tested to ensure they are secure against cyber attacks.[13]

Any changes to IRS systems should further account for the need to limit the use of the SSN as a ubiquitous identifier, a goal the IRS itself has acknowledged.[14] Reducing the use of SSNs will provide additional security and privacy to taxpayers, and help the IRS to protect sensitive information. We urge the committee to question the IRS about its intentions on this transition.

---

[5] U.S. Dep't Treasury Inspector Gen. for Tax Admin., *Annual Assessment of the Internal Revenue Service Information Technology Program* 24 (2017), https://www.treasury.gov/tigta/auditreports/2017reports/201720089fr.pdf [hereinafter *2017 OIG Report*].
[6] *Id.*
[7] Dave Rickard, *The Cost of 2017 Data Breaches*, CSO (Jan. 17, 2018), https://www.csoonline.com/article/3249088/data-breach/the-cost-of-2017-data-breaches.html.
[8] EPIC, *EPIC Student Privacy Project*, https://epic.org/privacy/student.
[9] U.S. Dep't Treasury Inspector Gen. for Tax Admin., *Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented* (2018), https://www.oversight.gov/sites/default/files/oig-reports/201820066fr.pdf.
[10] *2017 OIG Report*, *supra* note 5, at 27-28.
[11] Derek B. Johnson, *Audit Finds Another Cyber Headache for IRS*, FCW (June 25, 2018), https://fcw.com/articles/2018/06/25/irs-transcript-breach-fallout.aspx; *see also* U.S. Dep't Treasury Inspector Gen. for Tax Admin., *The Cybersecurity Data Warehouse Needs Improved Security Controls* (2018), https://www.treasury.gov/tigta/auditreports/2018reports/201820030fr.pdf.
[12] *Id.* at 31.
[13] *See, e.g.*, FedRAMP, *Penetration Testing for All FedRAMP Moderate and High Systems* (May 3, 2018), https://www.fedramp.gov/penetration-testing-for-all-fedramp-moderate-and-high-systems.
[14] Use of Truncated Taxpayer Identification Numbers on Forms W-2, 82 Fed. Reg. 43,920 (proposed Sept. 20, 2017), https://www.federalregister.gov/documents/2017/09/20/2017-19910/use-of-truncated-taxpayer-identification-numbers-on-forms-w-2-wage-and-tax-statement-furnished-to. EPIC supported this proposal, and filed comments with the IRS. Electronic Privacy Information Center, Comment on Request for Public Comment on Use of Truncated Taxpayer Identification Numbers on Forms W-2 (Dec. 18, 2017), https://epic.org/apa/comments/EPIC-IRS-SSN-Dec2017.pdf/EPIC-IRS-SSN-Dec2017.pdf.

Thank you for your attention to these critical issues. EPIC looks forward to working with the Subcommittee to ensure that taxpayers are protected online. We ask that this letter be entered in the hearing record.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Jeff Gary*
Jeff Gary
EPIC Legislative Fellow

October 10, 2018

The Honorable Lynn Jenkins, Chairman
The Honorable John Lewis, Ranking Member
Committee on Ways & Means, Subcommittee on Oversight
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Jenkins and Ranking Member Lewis:

On September 26, 2018 the Subcommittee held a hearing entitled, "IRS Taxpayer Authentication: Strengthening Security While Ensuring Access." We appreciate your focus on the IRS' taxpayer authentication procedures and look forward to working with you to make sure the system is secure, accessible and able to respond to a changing business environment.

The IRS Income Verification Express Service (IVES) serves a crucial role within the consumer and home lending process. Our associations represent institutions that use the service daily to verify consumers' financial information, thereby enabling financial institutions to extend credit to consumers. Our member institutions are committed to data security at every level and are pleased to partner with the IRS to protect our customers' data.

The IRS announced at the end of last year that new security protocols (known as Secure Access) would take effect within their broader e-Services platform. Our member institutions adapted their internal systems to comply with this new authentication process and engaged IRS leadership to address technical challenges and minimize disruptions to the credit markets.

The IRS' decision to implement Secure Access and ongoing efforts to redact certain personally identifiable information are strong steps to help protect the American taxpayer. Our member institutions have been discussing ways to improve the security of the IVES system while moving toward a modern, secure and fully integrated Business to Government (B2G) solution, as contemplated by HR 3860, the IRS Data Verification Modernization Act of 2017.

As the Subcommittee continues to examine taxpayer authentication procedures and process improvements, we encourage you to consider the creation of a secure, fully integrated and cost-effective B2G solution that can operate in our dynamic economy and protect against evolving threats. Our member institutions support a streamlined process that promotes efficiency while minimizing the burden on participants.

We support Congressional efforts to make investments in technology improvements at the IRS and are pleased to note the agency's leadership support for updating critical systems. An integrated, internet-based B2G solution for taxpayer authentication would be more beneficial for data security than a piecemeal approach.

Thank you for your continued work on this important issue and we welcome the opportunity to continue to discuss these issues with you moving forward.

Sincerely,

American Bankers Association
Consumer Bankers Association
Consumer Data Industry Association
Consumer Mortgage Coalition
Credit Union National Association
Housing Policy Council
Independent Community Bankers of America
Mortgage Bankers Association
National Association of Federally-Insured Credit Unions