

CAN THE IRS PROTECT TAXPAYERS' PERSONAL INFORMATION?

HEARING

BEFORE THE

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND
TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

April 14, 2016

Serial No. 114-72

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: <http://science.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

20-842PDF

WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma	EDDIE BERNICE JOHNSON, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin	ZOE LOFGREN, California
DANA ROHRBACHER, California	DANIEL LIPINSKI, Illinois
RANDY NEUGEBAUER, Texas	DONNA F. EDWARDS, Maryland
MICHAEL T. MCCAUL, Texas	SUZANNE BONAMICI, Oregon
MO BROOKS, Alabama	ERIC SWALWELL, California
RANDY HULTGREN, Illinois	ALAN GRAYSON, Florida
BILL POSEY, Florida	AMI BERA, California
THOMAS MASSIE, Kentucky	ELIZABETH H. ESTY, Connecticut
JIM BRIDENSTINE, Oklahoma	MARC A. VEASEY, Texas
RANDY K. WEBER, Texas	KATHERINE M. CLARK, Massachusetts
JOHN R. MOOLENAAR, Michigan	DON S. BEYER, JR., Virginia
STEVE KNIGHT, California	ED PERLMUTTER, Colorado
BRIAN BABIN, Texas	PAUL TONKO, New York
BRUCE WESTERMAN, Arkansas	MARK TAKANO, California
BARBARA COMSTOCK, Virginia	BILL FOSTER, Illinois
GARY PALMER, Alabama	
BARRY LOUDERMILK, Georgia	
RALPH LEE ABRAHAM, Louisiana	
DARIN LAHOOD, Illinois	

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. BARBARA COMSTOCK, Virginia, *Chair*

FRANK D. LUCAS, Oklahoma	DANIEL LIPINSKI, Illinois
MICHAEL T. MCCAUL, Texas	ELIZABETH H. ESTY, Connecticut
RANDY HULTGREN, Illinois	KATHERINE M. CLARK, Massachusetts
JOHN R. MOOLENAAR, Michigan	PAUL TONKO, New York
BRUCE WESTERMAN, Arkansas	SUZANNE BONAMICI, Oregon
GARY PALMER, Alabama	ERIC SWALWELL, California
RALPH LEE ABRAHAM, Louisiana	EDDIE BERNICE JOHNSON, Texas
DARIN LAHOOD, Illinois	
LAMAR S. SMITH, Texas	

CONTENTS

Thursday, April 14, 2016

Witness List	Page 2
Hearing Charter	3

Opening Statements

Statement by Representative Barbara Comstock, Chairwoman, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	7
Written Statement	9
Statement by Daniel Lipinski, Minority Ranking Member, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	11
Written Statement	13
Statement by Representative Lamar S. Smith, Chairman, Committee on Science, Space, and Technology, U.S. House of Representatives	16
Written Statement	17

Witness:

The Honorable John Koskinen, Commissioner, Internal Revenue Service	
Oral Statement	19
Written Statement	22
The Honorable J. Russell George, Inspector General, Treasury Inspector General for Tax Administration	
Oral Statement	39
Written Statement	41
Mr. Gregory Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office	
Oral Statement	55
Written Statement	57
Discussion	79

Appendix I: Answers to Post-Hearing Questions

The Honorable John Koskinen, Commissioner, Internal Revenue Service	104
The Honorable J. Russell George, Inspector General, Treasury Inspector General for Tax Administration	108
Mr. Gregory Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office	110

Appendix II: Slides

Document submitted by Representative Barbara Comstock, Chairwoman, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	114
Document submitted by Representative Barbara Comstock, Chairwoman, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	149

IV

	Page
Document submitted by Representative Barbara Comstock, Chairwoman, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	195
Statement submitted by Representative Eddie Bernice Johnson, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives	234

CAN THE IRS PROTECT TAXPAYERS' PERSONAL INFORMATION?

THURSDAY, APRIL 14, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittee met, pursuant to call, at 10:05 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Barbara Comstock [Chairwoman of the Subcommittee] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

Can the IRS Protect Taxpayers' Personal Information?

Thursday, April 14, 2016
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

The Honorable John Koskinen, Commissioner, Internal Revenue Service

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

Mr. Gregory Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office

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

HEARING CHARTER

Can the IRS Protect Taxpayers' Personal Information?

Thursday, April 14, 2016
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

On Thursday April 14, 2016, the Research & Technology Subcommittee will hold a hearing titled *Can the IRS Protect Taxpayers' Personal Information?* The purpose of the hearing is to review the Internal Revenue Service's (IRS) efforts to electronically authenticate the identity of taxpayers filing a tax return or accessing tax account services. In light of evolving cyber threats, the hearing will also review the IRS' compliance with information security standards and guidelines provided by the National Institute of Standards and Technology (NIST), as required by the Federal Information Security Management Act (FISMA). Additionally, the hearing will examine last year's unauthorized access of data from the IRS' Get Transcript application, and this year's hack of the Identity Protection Personal Identification Number (IP PIN) application. Both of these online applications were suspended by the agency because of security concerns.¹

Under FISMA, for non-Defense-related Federal agencies, NIST is tasked with "developing information security standards and guidelines, including minimum requirements for Federal information systems."² As part of this requirement, NIST provides "technical guidelines to agencies to allow an individual to remotely authenticate his or her identity to a Federal IT system."³ These guidelines supplement guidance provided by the Office of Management and Budget (OMB) to federal agencies "to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance."⁴

Witness List

- **The Honorable John Koskinen**, Commissioner, Internal Revenue Service
- **The Honorable J. Russell George**, Inspector General, Treasury Inspector General for Tax Administration
- **Mr. Gregory Wilshusen**, Director, Information Security Issues, U.S. Government Accountability Office

¹ Brian Krebs, "IRS Suspends Insecure 'Get IP PIN' Feature," Krebs on Security, March 16, 2016, available at: <http://krebsonsecurity.com/2016/03/irs-suspends-insecure-get-ip-pin-feature>.

² "Electronic Authentication Guideline," NIST Special Publication 800-63-2, August 2013, available at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>.

³ Ibid.

⁴ "E-Authentication Guidance for Federal Agencies," OMB Memorandum M-04-04, December 16, 2003, available at: <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>.

Background

Get Transcript

In January 2014, the IRS launched the online Get Transcript application to provide taxpayers with the ability to view, print, and download their tax transcript.⁵ A year later, on May 26, 2015, the IRS announced that criminals had used “taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information on approximately 100,000 tax accounts through IRS’ ‘Get Transcript’ application. This data included Social Security information, date of birth and street address.”⁶ At the time, the IRS claimed that approximately 100,000 taxpayers’ accounts had been accessed out of about 200,000 total attempts. Since then, those numbers have been revised to approximately 340,000 in August 2015, and as of this February, to over 700,000 taxpayers who have had their personal and tax data stolen.⁷

The theft of this data enabled the hackers to access information from prior tax returns, which in turn allowed them to file new and fraudulent tax returns. An estimated 15,000 of the fraudulent tax documents were successfully filed with the IRS leading to approximately \$50 million in refunds.⁸

IP PIN

The IRS began issuing IP PINS during the 2011 filing season to victims of identity theft.⁹ The IP PIN is a “6-digit number assigned to eligible taxpayers to help prevent the misuse of their Social Security number on fraudulent federal income tax returns.”¹⁰ The agency mails new IP PINS to taxpayers each year in late December or early January. In addition to identity theft victims, IP PIN recipients include individuals who participated in a pilot program for residents of Washington, DC, Florida, and Georgia.¹¹

On March 7, 2016, the IRS suspended the online IP PIN application amidst security concerns.¹² In one incident, a certified public accountant from South Dakota who received her IP PIN in 2014, found out that her number had been compromised when she tried to file her taxes on

⁵ Fact Sheet: Education Datapalooza to Promote Innovation in Improving College Access, Affordability, and Completion, January 15, 2014, available at:

https://www.whitehouse.gov/sites/default/files/docs/datapalooza_fact_sheet.pdf.

⁶ IRS Statement, May 26, 2015, available at: <https://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application>.

⁷ Brian Krebs, “IRS Suspends Insecure ‘Get IP PIN’ Feature,” Krebs on Security, March 16, 2016, available at: <http://krebsonsecurity.com/2016/03/irs-suspends-insecure-get-ip-pin-feature/>.

⁸ Keith Collins, “A Rare Detailed Look Inside the IRS’s Massive Data Breach, Via a Security Expert Who Was a Victim,” Quartz, August 27, 2015, available at: <http://qz.com/445233/inside-the-irss-massive-data-breach/>.

⁹ “There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft,” TIGTA Report, July 19, 2012, Reference Number: 2012-42-080, available at:

<https://www.treasury.gov/tigta/auditreports/2012reports/201242080ft.html>.

¹⁰ IRS website, available at: <https://www.irs.gov/Individuals/Frequently-Asked-Questions-about-the-Identity-Protection-Personal-Identification-Number-%28IP-PIN%29#q1>.

¹¹ IRS website, available at: <https://www.irs.gov/Individuals/Frequently-Asked-Questions-about-the-Identity-Protection-Personal-Identification-Number-%28IP-PIN%29#q14>.

¹² IRS Statement, March 7, 2016, available at: <https://www.irs.gov/uac/Newsroom/IRS-Statement-on-IP-PIN>.

February 25, 2016 -- someone had already filed a tax return under her name and account a few weeks earlier with a large refund request.¹³

According to the IRS, of the 2.7 million IP PINs issued to taxpayers for the current filing season, approximately 130,000 individuals used the online tool to try to retrieve a lost or forgotten IP PIN. Of that number, the IRS states that through the end of February 2016, it has confirmed and stopped 800 fraudulent returns using an IP PIN.¹⁴

Treasury Inspector General for Tax Administration (TIGTA) Report

Last year, TIGTA issued a report on the results of its review of the IRS' efforts to "authenticate individual taxpayers' identities at the time tax returns are filed and when obtaining services."¹⁵ TIGTA conducted the audit because failure "to adequately authenticate taxpayers filing a tax return and accessing tax account services can lead to identity theft. The increased availability of personal information warrants an assessment of the authentication risk across IRS services."¹⁶

TIGTA found that "authentication methods used for current online services do not comply with Government Information Security Standards. For example, TIGTA analysis of the e-Authentication processes used to authenticate users of the IRS online Get Transcript and Identity Protection Personal Identification Number applications found that the authentication methods provide only single-factor authentication despite the Government standards requiring multifactor authentication for such high-risk applications. As a result, unscrupulous individuals have gained unauthorized access to tax account information."¹⁷

However, the TIGTA report also notes that even the single-factor e-Authentication framework used by the IRS "does not meet NIST standards because it is unable to provide all of the functionality required by NIST standards for single-factor authentication."¹⁸

U.S. Government Accountability Office (GAO) Report

Last month, as part of its audit of "IRS's fiscal year 2015 and 2014 financial statements, GAO assessed whether controls over key financial and tax processing systems were effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information."¹⁹ The GAO report states that while the IRS "made progress in implementing information security controls...weaknesses in the controls limited their effectiveness in protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer data."²⁰

¹³ Brian Krebs, "Thieves Nab IRS PINs to Hijack Tax Refunds," Krebs on Security, March 16, 2016, available at: <http://krebsonsecurity.com/2016/03/thieves-nab-irs-pins-to-hijack-tax-refunds/>.

¹⁴ IRS Statement, March 7, 2016, available at: <https://www.irs.gov/uac/Newsroom/IRS-Statement-on-IP-PIN>.

¹⁵ "Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures are Needed," TIGTA Report, November 19, 2015, Reference Number: 2016-40-007, available at: <https://www.treasury.gov/tigta/auditreports/2016reports/201640007fr.pdf>.

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ Ibid.

¹⁹ "Information Security: IRS Needs to Further Improve Controls Over Financial and Taxpayer Data," GAO Report, March 2016, GAO-16-398, available at: <http://www.gao.gov/assets/680/676097.pdf>.

²⁰ Ibid.

The report further notes that:

“An underlying reason for these weaknesses is that IRS has not effectively implemented elements of its information security program. The agency had a comprehensive framework for its program, such as assessing risk for its systems, developing security plans, and providing employees with security awareness and specialized training. However, aspects of its program had not yet been effectively implemented. For example, IRS had not updated key mainframe policies and procedures to address issues such as comprehensively auditing and monitoring access. In addition, IRS did not include sufficient detail in its authorization procedures to ensure that access to systems was appropriate. Further, IRS had not ensured that many of its corrective actions to address previously identified deficiencies were effective. For example, for the 28 prior recommendations that IRS informed us that it had addressed, 9 of the associated weaknesses had not been effectively corrected.”²¹

Unless IRS takes steps to follow GAO’s recommendations, “its financial and taxpayer data will remain unnecessarily vulnerable to inappropriate and undetected use, modification, or disclosure.”²²

²¹ Ibid.

²² Ibid.

Chairwoman COMSTOCK. The Committee on Science, Space, and Technology will come to order.

Without objection, the Chair is authorized to declare recesses of the Committee at any time.

Good morning, and welcome to today's hearing titled "Can the IRS Protect Taxpayers' Personal Information?" I now recognize myself for five minutes for an opening statement.

As someone who, myself, received one of those IRS letters telling me that my tax information had been possibly compromised, as the deadline to file taxes winds down, you know, certainly the only question on taxpayers' minds should be when they will receive their tax refund and not whether someone else has already beaten them to it. You know, as I said, I received that letter actually last year informing me that my account may have been compromised, but recent news reports and audits of the Internal Revenue Service by the Treasury Inspector General for Tax Administration and the U.S. Government Accountability Office would suggest otherwise.

On May 26, 2015, the IRS announced that criminals had gained unauthorized access to taxpayer information through its online "Get Transcript" application by accurately answering taxpayers' security questions. At first, as it shut down the application, the IRS claimed that around 100,000 taxpayers' accounts had been accessed out of about 200,000 total attempts. Since then, those numbers have been revised to approximately 340,000 in August, and as of this February this year to over 700,000 taxpayers who have had their personal and tax data stolen. So I guess I'm in a lot of company.

The theft of this data enabled hackers to access information from prior tax returns, which resulted in fraudulent tax claims. Approximately 15,000 of the fraudulent tax claims were successfully filed with the IRS leading to an estimated \$50 million in illicit refunds—\$50 million in illicit refunds to people who have stolen information and who had no right to that \$50 million.

Then on March 7, 2016, the IRS suspended the Identity Protection Personal Identification Number—or IP PIN—application due to security concerns. The IRS began issuing IP PINS five years ago to victims of identity theft as an additional layer of security when they filed their taxes. But the system to protect the IP PIN application was the same as the "Get Transcript" application that was hacked last year. While the IRS suspended the "Get Transcript" application in May, it did not—May of last year—it did not suspend the IP PIN application until last month, during which time at least one individual had her taxpayer information stolen and used to file a fraudulent tax return.

I understand and sympathize with the frustrations of the American public and the hardworking taxpayers over these incidents. And what makes matters worse is that no one had to break into the IRS system to access information. Instead, the criminals used information from other cyber-attacks to accurately answer questions on the IRS website to access information they should not have been able to access, and may not have been able to access had the agency followed security guidelines provided by the National Institute of Standards and Technology. This ostensible lack of compliance with NIST guidelines is disconcerting, to say the least.

While I appreciate the IRS's efforts to accommodate most people's desire to access their tax information electronically, it cannot do so at the expense of their security. Again, as someone whose own information was possibly compromised, we never know in last year's OPM hack, I assure you, more security is better than less. This would also help many of my federal employee constituents who were impacted by the OPM breach, and I can tell you, as I go around to dozens and dozens of events and businesses, one of the first questions I ask them is, how many of you have had your information breached, how many of you have gotten those letters, because I've gotten two of them. I had my OPM information also breached. And it is rare that I don't have half of the hands at any meeting in my district go up, that they have had some type—they've gotten one of those letters from the government. As one of the largest health insurance providers in the Commonwealth, the Anthem hack also hit close to home for us.

I look forward to hearing from our witnesses today, and I thank you all again for being here.

[The prepared statement of Chairwoman Comstock follows:]



COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
April 14, 2016

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Research & Technology Subcommittee Chairwoman Barbara Comstock (R-Va.)
Can the IRS Protect Taxpayers' Personal Information?

Chairwoman Comstock: As the deadline to file taxes winds down, the only question on taxpayers' minds should be when they will receive their tax refund, and not whether someone else has already beaten them to it. I should know – I received a letter from the IRS earlier this year informing me that my account was compromised. But recent news reports and audits of the Internal Revenue Service by the Treasury Inspector General for Tax Administration, or TIGTA, and the U.S. Government Accountability Office (GAO) would suggest otherwise.

On May 26, 2015, the IRS announced that criminals had gained unauthorized access to taxpayer information through its online "Get Transcript" application by accurately answering taxpayers' security questions. At first, as it shut down the application, the IRS claimed that around 100,000 taxpayers' accounts had been accessed out of about 200,000 total attempts. Since then, those numbers have been revised to approximately 340,000 in August 2015, and as of this February, to over 700,000 taxpayers who have had their personal and tax data stolen.

The theft of this data enabled hackers to access information from prior tax returns which resulted in fraudulent tax claims. Approximately 15,000 of the fraudulent tax claims were successfully filed with the IRS leading to an estimated \$50 million in illicit refunds.

Then on March 7, 2016, the IRS suspended the Identity Protection Personal Identification Number – or IP PIN – application due to security concerns. The IRS began issuing IP PINs five years ago to victims of identity theft as an additional layer of security when they filed their taxes. But the system to protect the IP PIN application was the same as the "Get Transcript" application that was hacked last year.

While the IRS suspended the "Get Transcript" application in May, it did not suspend the IP PIN application until last month, during which time at least one individual had her taxpayer information stolen and used to file a fraudulent tax return.

I understand and sympathize with the frustrations of the American public over these incidents. And what makes matters worse is that no one had to break into the IRS system to access information. Instead, the criminals used information from other

cyber-attacks to accurately answer questions on the IRS website to access information they should not have been able to access, and may not have been able to access had the agency followed security guidelines provided by the National Institute of Standards and Technology (NIST).

This ostensible lack of compliance with NIST guidelines is disconcerting. While I appreciate the IRS' efforts to accommodate most people's desire to access their tax information electronically, it cannot do so at the expense of their security. As someone whose information was compromised in last year's OPM hack, I assure you, more security is better than less. This would also help many of my federal employee constituents who were impacted by the OPM breach, as well as by last year's Anthem cyber-attack. As one of the largest health insurance providers in the Commonwealth, the Anthem hack hit particularly close to home for us too.

I look forward to hearing from our witnesses and I thank you all again for being here today.

###

Chairwoman COMSTOCK. Before I recognize the Ranking Member, I would like to ask unanimous consent to enter into the record a couple of reports relevant to the hearing: one by the GAO and one by TIGTA. I also plan to submit my letter minus some of the personal information just so we have a sample of that. So without objection, so ordered.

[The information appears in Appendix II]

Chairwoman COMSTOCK. And I now recognize the Ranking Member, the gentleman from Illinois, Mr. Lipinski, for an opening statement.

Mr. LIPINSKI. Thank you Chairwoman Comstock for holding this hearing and welcome to the witnesses today. Today we'll be discussing cybersecurity breaches at two IRS online service portals.

Just about every American can expect to interact with the IRS during his or her life, and the agency's responsibilities make it privy to significant amounts of personal information about all of these individuals. Consequently, the data breaches at the IRS are particularly troubling and we should closely examine what the IRS has done wrong when it comes to protecting the personal information of Americans, how it can do better in regard to cybersecurity, and what Congress can do to better support IRS cybersecurity efforts. In meeting their obligation to pay taxes, Americans should have confidence that the IRS is taking all possible steps to protect them from cyber thieves.

Cybersecurity remains an evolving challenge across federal agencies as well as the private sector. Standards that were leading edge a year ago may be outdated today. Security is not a one-time goal to be achieved and placed on autopilot; it is a process that requires vigilance, continual learning, and fast dissemination of critical information to prevent and respond to new threats. While no entity, public or private, can protect data with 100 percent certainty, we must be nimble in learning from failures or missteps in cybersecurity policies and procedures.

To this end, we should heed the careful and detailed recommendations of the GAO and the Inspectors General. We must also ensure that decisions on cybersecurity policies are backed by a process that supports accountability, robust and forward-looking decision-making, and a clear sense of the consequences that can stem from data security failures.

Unfortunately, it is not at all apparent from the recent breaches at the IRS that the agency's policies were governed by such a comprehensive process. The two breaches that we are discussing today—the Get Transcript application and the Identity Protection PIN application—should not be viewed in isolation. Both of these breaches were facilitated in part by the same security weakness, namely the overreliance on out-of-the-wallet questions derived from credit report data. While in principle the answers to such questions should only be known by taxpayers, in practice they can often be guessed or uncovered from sources such as social media or websites compiling public record data. As a result, a breach in one application should have tipped off the IRS that the other was vulnerable as well. Yet the agency continued to make online IP PIN retrieval available long after shutting down the Get Transcript application because of security concerns. Further, the agency continued to do

so even after the Treasury Inspector General for Tax Administration warned the IRS to shut down the IP PIN tool as well.

We must get clarity on what steps the IRS is taking to ensure internal information sharing so that any breaches and their implications are quickly assessed across the entire organization and not just separate units or staff dealing directly with a problem at hand. Further, we must examine why the IRS ignored or deprioritized the TIGTA recommendation to shut down the IP PIN tool. Simply put, given how one breach built on the other, this should not have occurred.

In the context of this hearing, it is important to talk about NIST, an agency that this Subcommittee has jurisdiction over. NIST plays an important role in developing technical standards and providing expert advice to agencies across the government as they carry out their responsibilities under the Federal Information Security Management Act, or FISMA.

It is clear that the IRS did not follow the risk analysis or cybersecurity and authentication standards set by NIST when it set up these portals. The most important question is “why?” Was it a lacking—was it a lack of understanding of the standards? In this case, we need to have NIST here to talk about the standards and how to make them more clear. Or are there technical barriers to implementing the NIST standards at all? In this case, we need to have information on why these applications were allowed to go live in the first place. Or was this a strategic decision driven by tradeoffs between consumer convenience and security? These were put online to make the experience of taxpayers with the IRS better and easier. But if that’s the case, we must be clear: the IRS has a unique role among federal agencies and holds information on taxpayers that few others have. Protection of taxpayer data must be a top-level priority, and we must work to ensure that a breach of this nature doesn’t happen again.

Finally, I’d like to note that successful data security efforts depend on agencies being able to hire experienced cybersecurity professionals as well as having budgetary resources specifically directed toward security infrastructure. While some security failures at the IRS raise oversight questions about decision-making protocols at the management level, we also cannot ignore that successful implementation of good security practices costs money. Although this is beyond the scope of our Committee’s jurisdiction, I am concerned that Congress has yet to reauthorize IRS’s streamlined critical pay authority which helps the agency compete with the private sector for top cybersecurity talent. And as Congress makes funding decisions for the coming fiscal year, we must ensure that we provide resources to match current IT-specific needs.

I look forward to this morning’s discussion, and I yield back the balance of my time

[The prepared statement of Mr. Lipinski follows:]

OPENING STATEMENT
Ranking Member Daniel Lipinski (D-IL)
of the Subcommittee on Research and Technology

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
"Can the IRS Protect Taxpayers' Personal Information?"
April 14, 2016

Thank you Chairwoman Comstock for holding this hearing, and welcome to the witnesses. I know this is a busy season for you, and I appreciate you taking the time to appear before us this morning.

Today, we will be discussing cybersecurity breaches at two IRS online service portals. This hearing follows the reports of unauthorized access to the personal information of more than 700,000 American taxpayers, and the theft of money from taxpayers that likely came about as a result. Just about every American can expect to interact with the IRS during his or her life, and the agency's responsibilities make it privy to significant amounts of personal information about all of these individuals. Consequently, data breaches at the IRS are particularly troubling and we should closely examine what IRS has done wrong when it comes to protecting the personal information of Americans, how it can do better in regard to cybersecurity, and what Congress can do to better support IRS cybersecurity efforts. In meeting their obligation to pay taxes, Americans should have confidence that the IRS is taking all possible steps to protect them from cyber thieves.

Cybersecurity remains an evolving challenge across federal agencies as well as the private sector. Standards that were leading edge a year ago may be outdated today. Security is not a one-time goal to be achieved and placed on autopilot; it is a process that requires vigilance, continual learning, and fast dissemination of critical information to prevent and respond to new threats. While no entity, public or private, can protect data with 100% certainty, we must be nimble in learning from failures or missteps in cybersecurity policies and procedures. To this end, we should heed the careful and detailed recommendations of the GAO and the Inspectors General. We must also ensure that decisions on cybersecurity policies are backed by a process that supports accountability, robust and forward-looking decision-making, and a clear sense of

the consequences that can stem from data security failures. Unfortunately, it is not at all apparent from the recent breaches at the IRS that the agency's policies were governed by such a comprehensive process. The two breaches that we are discussing today – the Get Transcript application and the Identity Protection PIN application – should not be viewed in isolation. Both of these breaches were facilitated in part by the same security weakness, namely the overreliance on out of the wallet questions derived from credit report data. While in principle the answers to such questions should only be known by taxpayers, in practice they can often be guessed or uncovered from sources such as social media or websites compiling public record data. As a result, a breach in one application should have tipped off the IRS that the other was vulnerable as well. Yet the agency continued to make online IP PIN retrieval available long after shutting down the Get Transcript application because of security concerns. Further, the agency continued to do so even after the Treasury Inspector General for Tax Administration, or TIGTA, warned the IRS to shut down the IP PIN tool as well. We must get clarity on what steps the IRS is taking to ensure internal information sharing so that any breaches and their implications are quickly assessed across the entire organization and not just separate units or staff dealing directly with a problem at hand. Further, we must examine why the IRS ignored or deprioritized the TIGTA recommendation to shut down the IP PIN tool. Simply put, given how one breach built on the other, this should not have occurred.

In the context of this hearing it is important to talk about NIST, an agency that this subcommittee has jurisdiction over. NIST plays an important role in developing technical standards and providing expert advice to agencies across the government as they carry out their responsibilities under the Federal Information Security Modernization Act, or FISMA. It is clear that the IRS did not follow the risk analysis or cybersecurity and authentication standards set by NIST when it set up these portals. The most important question is “why?” Was it a lack of understanding of the standards? In this case, we need to have NIST here to talk about the standards and how to make them clearer. Or are there technical barriers to implementing the NIST standards at all? In this case, we need to have information on why these applications were allowed to go live in the first place. Or was this a strategic decision driven by tradeoffs between consumer convenience and security? In that case, we must be clear: the IRS has a unique role among federal agencies

and holds information on taxpayers that few others have. Protection of taxpayer data must be a top-level priority and we must work to ensure that a breach of this nature never happens again.

Finally, I would like to note that successful data security efforts depend on agencies being able to hire experienced cybersecurity professionals as well as having budgetary resources specifically directed toward security infrastructure. While some security failures at the IRS raise oversight questions about decision-making protocols at the management level, we also cannot ignore that successful implementation of good security practices costs money. Although this is beyond the scope of our Committee's jurisdiction, I am concerned that Congress has yet to reauthorize IRS' streamlined critical pay authority which helps the agency compete with the private sector for top cybersecurity talent. And as Congress makes funding decisions for the coming fiscal year, we must ensure that we provide resources to match current IT-specific needs.

I look forward to this morning's discussion, and I yield back the balance of my time.

Chairwoman COMSTOCK. Thank you, and I now recognize the chairman of the full Committee, Mr. Smith.

Chairman SMITH. Thank you, Madam Chair, and I appreciate the witnesses being here today.

In this Congress, the Science Committee has held half a dozen hearings on cybersecurity issues and vulnerabilities at federal agencies, and we continue to hear the concerns of millions of Americans who quite frankly don't trust the federal government to protect their personal information from cyber criminals. Too many federal agencies fail to meet the basic standards of information security. We've seen this with HealthCare.Gov and the cyber breach at the Office of Personnel Management. The same is true for the IRS.

According to a report published last November by the Treasury Inspector General for Tax Administration), the IRS's identity authentication methods for online services do not comply with Government Information Security Standards. In other words, the IRS has not taken the necessary steps to ensure that individuals are who they claim to be before handing over Americans' confidential tax information. As a result of these vulnerabilities, the TIGTA report found that, "unscrupulous individuals have gained unauthorized access to tax account information."

The U.S. Government Accountability Office has identified a number of ongoing cybersecurity system gaps and IRS failures to fully implement certain security controls. The report found that of 28 prior GAO cybersecurity recommendations to the IRS, nine have not been effectively implemented. These gaps could open the door for cyber criminals to steal confidential taxpayer data.

The past year's IRS breaches are especially troubling. Taxpayer data was fraudulently accessed, not through a forcible compromise of the computer systems, but by hackers who correctly answered security questions that should have only been answerable by the actual individual. The hackers likely accessed the requisite data from prior high-profile hacks.

Last year's OPM and Anthem Health Insurance breaches compromised the information of over 100 million people. This included the names, addresses, dates of birth, and Social Security numbers of the victims. For cyber criminals, this information is similar to making duplicate keys to your house. It's a license to steal whenever and wherever the criminals find an opportunity.

The IRS security breach demonstrates once again that rigorous adherence to all cybersecurity protections must be the top priority for every federal agency. Slow responses and partial measures at the IRS do not protect innocent Americans from these cyber-attacks. The government should be accountable to the people and keep Americans' sensitive information secure.

Thank you, Madam Chairman, and I'll yield back.

[The prepared statement of Chairman Smith follows:]



COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
April 14, 2016

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Chairman Lamar Smith (R-Texas)
Can the IRS Protect Taxpayers' Personal Information?

Chairman Smith: Thank you Madam Chair, and thanks to our witnesses for being here today.

In this Congress, the Science Committee has held half a dozen hearings on cybersecurity issues and vulnerabilities at federal agencies. And we continue to hear the concerns of millions of Americans who quite frankly don't trust the federal government to protect their personal information from cyber criminals.

Too many federal agencies fail to meet the basic standards of information security. We've seen this with HealthCare.Gov and the cyber breach at the Office of Personnel Management (OPM).

The same is true for the IRS. According to a report published last November by the Treasury Inspector General for Tax Administration (TIGTA), the IRS' identity authentication methods for online services do not comply with Government Information Security Standards.

In other words, the IRS has not taken the necessary steps to ensure that individuals are who they claim to be before handing over Americans' confidential tax information. As a result of these vulnerabilities, the TIGTA report found that, "unscrupulous individuals have gained unauthorized access to tax account information."

The U.S. Government Accountability Office (GAO) has identified a number of ongoing cybersecurity system gaps and IRS failures to fully implement certain security controls. The report found that of 28 prior GAO cybersecurity recommendations to the IRS, nine have not been effectively implemented.

These gaps could open the door for cyber criminals to steal confidential taxpayer data.

The past year's IRS breaches are especially troubling. Taxpayer data was fraudulently accessed, not through a forcible compromise of the computer systems, but by hackers who correctly answered security questions that should have only been answerable by the actual individual.

The hackers likely accessed the requisite data from prior high profile hacks. Last year's OPM and Anthem Health Insurance breaches compromised the information of over 100 million people. This included the names, addresses, dates of birth, and Social Security numbers of the victims.

For cyber criminals, this information is similar to making duplicate keys to your house. It's a license to steal whenever and wherever the criminals find an opportunity. The IRS security breach demonstrates once again that rigorous adherence to all cybersecurity protections must be the top priority for every federal agency.

Slow responses and partial measures at the IRS do not protect innocent Americans from these cyber-attacks. The government should be accountable to the people and keep Americans' sensitive information secure.

Thank you and I yield back.

###

Chairwoman COMSTOCK. Thank you.

And now I will introduce our witnesses. Our first witness today is the Honorable John Koskinen, 48th Commissioner of the Internal Revenue Service. Prior to his appointment, he served in executive roles at Freddie Mac and 21 years in the private sector in various leadership positions. He received his bachelor's degree from Duke University and a law degree from Yale. He also studied international law for one year in Cambridge, England.

Our second witness today is the Honorable Russell George, Treasury Inspector General for Tax Administration. Prior to his confirmation by the Senate in 2004, Mr. George served as the Inspector General of the Corporation for National and Community Service. His government service also includes working at the White House Office of Management and Budget as Assistant General Counsel, and working here in Congress as Staff Director and Chief Counsel of the then-named Government Management Information and Technology Subcommittee. Mr. George received his bachelor of arts degree from Howard University and his doctorate of jurisprudence from Harvard University's School of Law.

Our third and final witness today is Mr. Gregory Wilshusen. Mr. Wilshusen is the Director of Information Security Issues at the Government Accountability Office, where he leads cybersecurity and privacy-related studies and audits of the federal government in critical infrastructure. Prior to joining GAO in 1997, he held a variety of public- and private-sector positions. He is a certified public accountant, certified internal auditor, and certified information systems auditor. He received his bachelor of science degree in business administration from the University of Missouri and his master of science and information management from George Washington University.

I now recognize the IRS Commissioner for five minutes to present his testimony.

**TESTIMONY OF THE HONORABLE JOHN KOSKINEN,
COMMISSIONER, INTERNAL REVENUE SERVICE**

Mr. KOSKINEN. Thank you, Chairman Smith, Chairwoman Comstock, Ranking Member Lipinski, and members of the Subcommittee. I appreciate the opportunity to discuss with you today the IRS's ongoing efforts in regard to cybersecurity and identity theft. Securing our systems and taxpayer data continues to be a top priority for the IRS. Even with our constrained resources as a result of repeatedly decreased funding over the past few years, we continue to devote significant time and attention to this challenge. We work continuously to protect our main computer systems from cyber-attacks and to safeguard taxpayer information stored in our databases. These systems withstand more than one million attempts to access them each day.

We're also continuing to battle a growing problem of stolen identity refund fraud. Over the past few years, we've made steady progress in protecting against fraudulent refund claims and criminally prosecuting those who engage in this crime.

But we've found the type of criminal we are dealing with has changed. This problem used to be random individuals filing a few dozen or a few hundred false tax returns at a time. Now we're deal-

ing more and more with organized-crime syndicates here and in other countries. They're gathering unimaginable amounts of personal data as noted from sources outside the IRS so they can do a better job of impersonating taxpayers, evading our return processing filters, and obtaining fraudulent refunds.

To improve our efforts against this complex and evolving threat, in March 2015 we joined with the leaders of the electronic tax industry and the private sector, the software industry and the states to create the Security Summit Group. This is an unprecedented partnership that is focused on making the tax filing experience safer and more secure for taxpayers in 2016 and beyond.

Our collaborative efforts with the private sector and state tax commissioners have already shown concrete results this filing season. For example, Security Summit partners have helped us improve our ability to spot potentially false returns before they are processed. Over the past year, we've seen three examples of what identity thieves are capable of and why we can't let up in this fight. In each case we detected and stopped unauthorized attempts to access online services on our website, IRS.gov, by criminals masquerading as legitimate taxpayers. One of the services targeted, as noted, was our "Get Transcript" online application used by taxpayers to quickly obtain a copy of their prior year return. Another, as noted, was the online tool to retrieve lost identity protection personal identifier numbers, or IP PINs. Taxpayers who previously were victims of identity theft used these PINs to prove their identity when they filed a return. And the third was a tool that some people used to generate a PIN number when they e-filed their tax returns. In all three cases, criminals were trying to use our online tools to help them pretend to be legitimate taxpayers and sneak past false returns past our fraud filters. These incidents, which unfortunately in the case of "Get Transcript" access, resulted in the loss of taxpayer information for thousands of taxpayers before the application was disabled, has shown us that improving our reaction time to suspicious activity isn't enough. We need to be able to anticipate the criminals' next moves and attempt to stay ahead of them. The ongoing work of the Security Summit Group will be critical to our success here.

As we confront the challenge of identity theft, we're also working to expand and improve our ability to interact with taxpayers online to meet taxpayers' increasing demand for digital services. We are aware, however, that in building toward this enhanced online experience, we must continually upgrade and improve our ability to verify the identity of taxpayers using these services. Taxpayers will only use these services if they're confident that they are safe and secure. So we're in the process of developing a strong, coordinated authentication framework.

We have a delicate balance to maintain here. We need to keep the criminals out while letting the legitimate taxpayers in. Our goal is to have the strongest possible authentication process for our ongoing services while maintaining the ability of taxpayers to access their data and use IRS services online.

Congress can provide critical support by providing adequate resources for these efforts. We appreciate the \$290 million in additional funding Congress provided for fiscal 2016, which included

funds to improve cybersecurity and fight identity theft. We used over \$100 million of that funding and are using it now in those areas. Sustaining and increasing funding in this area will be critical as we move forward.

Another way Congress can help us is by passing legislative proposals to improve tax administration and cybersecurity. One of the most important requests we have made is for the reauthorization of streamlined critical pay, the loss of which has made it very difficult, if not impossible, to recruit and retain employees with expertise in highly technical areas such as information technology.

Chairman Smith, Chairwoman Comstock, Ranking Member Lipinski, and members of the Subcommittee, this concludes my statement. I'd be happy to take your questions.

[The prepared statement of Mr. Koskinen follows:]

**WRITTEN TESTIMONY OF
JOHN A. KOSKINEN
COMMISSIONER
INTERNAL REVENUE SERVICE
BEFORE THE
HOUSE SCIENCE, SPACE AND TECHNOLOGY COMMITTEE
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
ON CYBERSECURITY AND PROTECTING TAXPAYER INFORMATION
APRIL 14, 2016**

INTRODUCTION

Chairwoman Comstock, Ranking Member Lipinski and members of the Subcommittee, thank you for the opportunity to discuss the IRS's ongoing efforts to safeguard our systems and protect taxpayer information from cybersecurity threats, as well as our work to combat stolen identity refund fraud.

Securing our systems and taxpayer data continues to be a top priority for the IRS. Even with our constrained resources as a result of repeatedly decreased funding over the past few years, we continue to devote significant time and attention to this challenge, which is twofold.

First, the IRS works continuously to protect our main computer systems from cyber incidents, intrusions and attacks, but our primary focus is to prevent criminals from accessing taxpayer information stored in our databases. These core tax processing systems remain secure, through a combination of cyber defenses, which currently withstand more than one million attempts to maliciously access our systems each day. Second, the IRS is waging an ongoing battle to protect taxpayers and their information as we confront the growing problem of stolen identity refund fraud. Our multipronged approach to this problem is discussed in more detail below.

As we confront these challenges, the IRS has also been working to expand and improve our ability to interact with taxpayers online. While we already engage taxpayers across numerous communications channels, we realize the need to meet taxpayers' increasing demand for digital services.

We are aware, however, that in building toward this enhanced online experience, we must continuously upgrade and improve our authentication protocols. The reality is criminals are becoming increasingly sophisticated and are gathering vast amounts of personal information as the result of data breaches at sources outside the IRS. We must balance the strongest possible authentication processes with the ability of taxpayers to legitimately access their data and use IRS services online. It is important to note that cybercrime (theft by unauthorized

access) and privacy breaches are increasing across the country in all areas of government and industry. Cyber criminals and their methods continue to grow in sophistication, frequency, brazenness, volume and impact. IRS will continue to be challenged in our ability to maintain currency with latest technologies, processes and counter-measures.

MAKING PROGRESS AGAINST IDENTITY THEFT

Discovering that your identity has been stolen by having your tax return rejected because someone else has already filed a return using your name and Social Security Number (SSN) can be a personal and traumatic experience. We are constantly working to improve our processes and methods to protect taxpayers from this situation. The problem of personal data being used to file fraudulent tax returns and illegally obtain refunds exploded from 2010 to 2012, and for a time overwhelmed private industry, law enforcement, and government agencies such as the IRS. Since then, we have been making steady progress within our reduced resources, both in terms of protecting against fraudulent refund claims and criminally prosecuting those who engage in this crime.

Thanks to the work of our Criminal Investigation Division, about 2,000 individuals have been convicted on federal charges related to refund fraud involving identity theft over the past few years. We currently have about 1,700 open investigations being worked by more than 400 IRS criminal investigators.

Meanwhile, we continue to improve our efforts at stopping fraudulent refunds from going out the door. For example, we have improved the filters that help us spot suspicious returns before they can be processed. Using those filters, we stopped 1.4 million returns last year that were confirmed to have been filed by identity thieves. By stopping those returns, we kept criminals from collecting about \$8.7 billion in fraudulent refunds.

Importantly, the IRS also continues to help taxpayers who have been victims of identity theft. Last year, the IRS worked with victims to close more than 700,000 such cases.

But while we have stopped many crimes, we find that the type of criminal we are dealing with constantly evolves. Previously we were dealing with individuals stealing personal information and filing a few dozen or maybe a few hundred false tax returns, and while we still see this, the threat has grown to include organized crime syndicates here and in other countries.

Security Summit Group

To improve our efforts against this complex and evolving threat, the IRS held a sit-down meeting in March 2015 with leaders of the electronic tax industry,

software industry and state tax officials. We agreed to build on our past cooperative efforts and find new ways to leverage our public-private partnership to help battle stolen identity refund fraud. Motivating us was the understanding that no single organization can fight this type of fraud alone.

This meeting led to the development of the Security Summit group, an unprecedented partnership that has focused our joint efforts on making sure the tax filing experience would be safer and more secure for taxpayers in 2016 and beyond. This is an important step for taxpayers and for tax administration, because the critical work being done by this group is giving everyone involved a better defense against stolen identity refund fraud.

Over the past year, the Security Summit group has made progress on a number of initiatives including:

- Summit group members identified and agreed to share 20 data components from Federal and state tax returns to improve fraud detection and prevention this filing season. For example, group members are sharing computer device identification data tied to the return's origin, as well as the improper or repetitive use of the numbers that identify the Internet "address" from where the return originates.
- Tax software providers agreed to enhance identity requirements and strengthen validation procedures for new and returning customers to protect their accounts from being taken over by criminals. This change is one of the most visible to taxpayers during the 2016 filing season, because it includes new verification procedures they need to follow to log in to their accounts. These actions will serve as the baseline for ongoing discussions and additional enhancements for the 2017 filing season.
- The Summit group created a new memorandum of understanding (MOU) regarding roles, responsibilities and information sharing pathways currently in circulation with states and industry. So far, 40 state departments of revenue and 21 tax industry members have signed the MOU, along with the IRS and endorsing organizations.
- Tax industry participants have aligned with the IRS and the states under the National Institute of Standards and Technology (NIST) cybersecurity framework to promote the protection of information technology infrastructure. The IRS and states currently operate consistently with this framework, as do many in the tax industry. Next steps in this area include follow-up sessions to develop strategy for how the NIST cybersecurity framework will be employed by all organizations within the tax industry.
- Summit group members agreed on the need to create a tax administration Information Sharing and Analysis Center (ISAC) to centralize, standardize,

and enhance data compilation and analysis to facilitate sharing actionable data and information.

- Recognizing the critical role that the nation's tax professionals play within the tax industry in both the Federal and state arenas, the Summit group created a team that will examine issues related to return preparers, such as how the preparer community can help prevent identity theft and refund fraud.

Our collaborative efforts are already showing concrete results this filing season. For example, Security Summit partners have helped the IRS improve its ability to spot potentially false returns before they are processed and thus before a possibly fraudulent refund is issued. Under our industry leads program, Security Summit partners and other external stakeholders such as banks provide information that allows us to improve our fraud filters, which in turn leads to more suspicious returns being identified for further review. In Calendar Year (CY) 2016 through mid-March, leads from industry partners directly resulted in the suspension of 27,000 returns on which a total of \$119 million in refunds was claimed, up from 8,000 returns claiming \$57 million during the same period last year.

Identity Theft Public Awareness Campaign

Despite the progress being made against stolen identity refund fraud, we recognized that we were missing an important partner in this effort – the taxpaying public. So in November 2015, with the strong support of all the Security Summit partners, we launched the “Taxes, Security, Together” campaign to raise awareness about actions people can take to protect themselves and avoid becoming victims of identity theft.

Many of the steps are basic common sense, but given that 150 million households file tax returns every year, we believe these steps cannot be stressed enough. People continue to fall prey to clever cybercriminals who trick them into giving up SSNs, bank account numbers, password information or other sensitive personal data. So having the public's help will greatly strengthen and improve our new tools we have to stop the crime of identity theft.

As part of this public awareness campaign, the IRS, in the weeks leading up to the 2016 filing season, issued weekly tax tips describing the actions people could take to protect their data. We have updated several publications for taxpayers and tax professionals. We have posted YouTube videos on this subject, and public-awareness information is being shared online across IRS.gov, state websites and platforms used by the tax software industry and many others in the private-sector tax community. I would note our public awareness campaign is not confined to the tax filing season, but is an ongoing effort.

Our efforts to educate and inform members of the public about the need to protect themselves against identity thieves extend to businesses as well. Information returns, especially Form W-2, are becoming a major target of these criminals, as they seek new sources of information that will help them file false returns that have a better chance of going undetected by our fraud filters. In this effort, they attempt to trick companies into providing the information returns.

One scheme uncovered recently involved identity thieves posing as a company's chief executive and sending a legitimate-looking email to the payroll department requesting a list of all company employees and their Forms W-2. In March, the IRS issued an alert to payroll and human resources professionals warning them about this scam.

Identity thieves' efforts to obtain Forms W-2 have not stopped there. We are increasingly concerned about efforts to create counterfeit Forms W-2 that are filed along with the false returns to make the return appear legitimate. That concern led the IRS to launch a pilot program earlier this year testing the idea of adding a verification code to Form W-2 that would verify the integrity of Form W-2 data being submitted to the IRS.

For this pilot, the IRS partnered with four major payroll service providers. These providers added a special coded number on approximately 2 million individual Forms W-2 in a new box on the Form W-2 labeled "Verification Code." Each coded number is calculated based on a formula and key provided by the IRS, using data from the Form W-2 itself, so that each number generated was known only to the IRS, the payroll service provider, and the individual who received the Form W-2. The verification code cannot be reverse engineered. Since this identifier is unique, any changes to the Form W-2 information provided when filed are detected by the IRS. Individuals whose Forms W-2 were affected by the pilot and who used tax software to prepare their return entered the code when prompted to by the software program. The IRS plans to increase the scope of this pilot for the 2017 filing season by expanding the number and types of Form W-2 issuers involved in the test.

VERIFYING IDENTITIES AND STOPPING SUSPICIOUS ONLINE ACTIVITY

Following the OMB Guidance and NIST Standards

The IRS continues to make every effort to ensure that we provide tax account-related services only after verifying the identity of individuals seeking those services. This is true for all of our communications channels, some of which allow for extremely strong assurance processes that are not possible in other channels.

For example, IRS employees at our Taxpayer Assistance Centers provide face-to-face help to taxpayers, and thus can easily verify identity through photo identification. This method provides the strongest possible level of assurance, but is obviously not feasible with phone or online interactions. Additionally, in-person assistance is more time-consuming for the taxpayer and costly for the IRS than the help we provide through other communications channels.

Given the ability of cybercriminals and identity thieves to evolve and improve their methods of stealing personal data, the need to properly verify the identity of taxpayers using online services is particularly great. In developing authentication procedures for online interactions with taxpayers, the IRS continues to follow the Office of Management and Budget (OMB) memorandum issued in 2003, *E-Authentication for Federal Agencies*.

This memorandum establishes criteria for determining the risk-based level of authentication assurance required for specific electronic applications and transactions. It requires agencies to review new and existing electronic transactions, to ensure authentication processes provide the appropriate level of assurance from among four levels, which are as follows:

Level 1: Little or no confidence in the asserted identity's validity;
 Level 2: Some confidence in the asserted identity's validity;
 Level 3: High confidence in the asserted identity's validity; and
 Level 4: Very high confidence in the asserted identity's validity.

Each increase in level requires users to take additional steps to validate their identity and gain access to a given online transaction.

In addition to the OMB memorandum, we also follow the technical requirements set by NIST for the four levels of assurance defined in the OMB guidance. It is important to note that the NIST standards anticipate and require varying levels of assurance depending on the nature of a given online transaction and the information being exchanged.

In following the NIST standards, the IRS employs differing levels of authentication assurance among the various digital services used by taxpayers. For example, the level of authentication required for an online tool that only accepts payments from a taxpayer can reasonably be set lower than an application that provides the taxpayer with their personal tax information.

Thus, in establishing a risk assurance level to a particular online digital service, the IRS, in addition to assigning one of the four numerical levels of risk assurance, also assigns a letter representing the amount and types of validation that a taxpayer would have to provide, in order to gain access to the digital service in question:

- A: No credential required (OMB Level 1);
- B: User ID and password required, but no identity proofing (OMB Level 1);
- C: User ID and password, plus basic identity proofing – providing information such as name, address, date of birth, SSN (OMB Level 2);
- D: Everything included in C above, plus knowledge-based authentication – answers to so-called “out of wallet” questions that only the legitimate taxpayer should know (OMB Level 2);
- E: Everything included in D above, plus financial validation, such as providing the taxpayer’s prior-year adjusted gross income (OMB Level 2);
- F: Everything included in C above, plus financial validation and an additional authentication factor, such as an authentication code texted or mailed to the user – so-called multifactor identification (OMB Level 3); and
- G: In-person authentication.

Recent Unauthorized Attempts to Access IRS Online Services

Over the past year, unauthorized attempts were made to access online services on our website, IRS.gov. These attempts were not on our main computer system, which remains secure. Instead, in each situation criminals were attempting to use taxpayer information they had stolen from other sources to access IRS services by impersonating legitimate taxpayers, in order to file false tax returns and claim fraudulent refunds.

Each of the situations, which are described in more detail below – involving the Get Transcript online application, the Identity Protection Personal Identification Number (IP PIN) retrieval tool and the Get Your Electronic Filing PIN tool– illustrate both the progress we have made and the challenges we continue to face in detecting suspicious activity and ensuring the digital services we provide are used only by taxpayers who legitimately seek them.

For all three services, the improvements made to our system-monitoring capabilities allowed the IRS to uncover the suspicious activity. We continue to improve these monitoring capabilities and enhance our return processing filters so that we can thwart criminal activity as quickly as possible.

But improving our ability to react to these threats is not enough. The three situations are examples of how nimble criminals have become in attempting to access our systems by masquerading as legitimate taxpayers. In each case, those who were making the unauthorized attempts to gain access had already obtained vast amounts of stolen individual taxpayer data and were using it to help them get into our systems, with the ultimate goal of claiming a fraudulent refund. We are finding that, as the IRS improves monitoring capabilities and shuts off certain avenues of entry, identity thieves find new ways to file false returns. As the IRS enhances return processing filters and catches more fraudulent returns at the time of filing, criminals have become more sophisticated

at faking taxpayers' identities so they can evade those filters and successfully obtain fraudulent refunds.

Therefore, the IRS is working not just to react better and faster, but to anticipate the criminals' next moves and stay ahead of them. To fully protect taxpayers and the tax system, the IRS must not only keep pace with, but also get ahead of, criminals and criminal organizations, as they improve their efforts to obtain personal taxpayer information. The ongoing collaborative work of the Security Summit group along with additional funding received in FY 2016 as part of the Section 113 Administrative Provision have been crucial. The FY 2017 budget requests additional funding including a Departmentally-managed Cybersecurity Enhancement account which allows the IRS and the Department to leverage enterprise-wise services and capabilities.

Following are descriptions of the three situations referenced above involving suspicious online activity:

Get Transcript Application. The Get Transcript online application allows taxpayers to view and print a copy of their prior-year tax information, also known as a transcript, in a matter of minutes. Taxpayers use tax transcript information for a variety of non-tax administration, financial activities, such as verifying income when applying for a mortgage or financial aid.

Prior to the introduction of this online tool in January 2014, taxpayers needing a transcript had to order a transcript by mail, by phone, or in person at one of our Taxpayer Assistance Centers, and then have it mailed to them.

The development of the Get Transcript online application began in 2011. The IRS conducted a risk assessment and determined that the e-authentication risk assurance level appropriate for this application was 2D, which required the taxpayer to provide basic items of personal information and also answer out-of-wallet questions. At that time, this type of authentication process was the industry standard, routinely used by financial institutions to verify the identity of their customers conducting transactions online.

During the 2015 filing season, taxpayers used the Get Transcript online application to successfully obtain approximately 23 million transcripts. If this application had not existed and these taxpayers had to call or write us to order a transcript, it would have stretched the IRS's limited resources even further.

In May 2015, the IRS announced that criminals, using taxpayer information stolen elsewhere, had been able to access the Get Transcript online application. Shortly thereafter, we disabled the application. We are now strengthening the authentication process and expect to bring the Get Transcript application back on-line, in the near future. In reevaluating the application, we have changed the risk assurance level for this application to 3F, which will require taxpayers to

undergo a multifactor authentication process in order to gain access. In the meantime, taxpayers can still place an order for a transcript online, and have it mailed to their address of record.

The IRS, immediately focusing on last year's filing season, initially identified approximately 114,000 taxpayers whose transcripts had been accessed and approximately 111,000 additional taxpayers whose transcripts were targeted but not accessed. We offered credit monitoring, at our expense, to the group of 114,000 for which the unauthorized attempts at access were successful. We also promptly sent letters to all of these taxpayers to let them know that third parties may have obtained their personal information from sources outside the IRS in an attempt to obtain their tax return data using the Get Transcript online application.

Our review of the situation continued and, in August 2015, we identified another 220,000 taxpayers whose transcripts may have been accessed and approximately 170,000 taxpayers whose transcripts were targeted but not accessed. We again notified all of these taxpayers about the unauthorized attempts, and offered credit monitoring to the 220,000.

In addition, the Treasury Inspector General for Tax Administration (TIGTA) conducted a nine-month investigation looking back to the launch of the application in January 2014 for additional suspicious activity. This expanded review identified additional unauthorized attempts to access taxpayer information using the Get Transcript online application. This review found potential access of approximately 390,000 additional taxpayer accounts during the period from January 2014 through May 2015. An additional 295,000 taxpayer transcripts were targeted but access was not successful. Again, the IRS sent letters to these taxpayers alerting them to the unauthorized attempts, offering credit monitoring to those whose accounts were accessed.

The additional attempts uncovered by TIGTA brought the total number of potential unauthorized accesses to the Get Transcript online application to 724,000. So far, we have identified approximately 250,000 potentially fraudulent returns that were filed on behalf of these taxpayers, and we have stopped the majority of the known fraudulent refunds from going out.

I would note that our analysis of the attempts to access the Get Transcript online application is ongoing, and we may yet discover that some accesses classified as unauthorized were, in fact, legitimate. For example, family members, tax return preparers or financial institutions could have been using a single email address to attempt to access more than one account. However, in an abundance of caution, IRS notified any and all taxpayers whose accounts met these criteria.

Additionally, as a result of the Get Transcript online application problem, we added an extra layer of protection for taxpayers who use our online services. We

started sending a letter, known as a CP301 notice, to taxpayers when they first create a login and password for any web application on IRS.gov. This notice tells the taxpayer that someone registered for an IRS online service using their information. If the taxpayer was not the one who registered, the notice instructs the taxpayer to contact the IRS. Mailing this notice conforms to NIST guidance, and is a best practice similar to that used by the Social Security Administration and other financial institutions.

Since we began sending these notices, we have disabled approximately 5,100 online accounts at the request of taxpayers who received a CP301. The majority of these accounts were disabled between January and March of this year, and we estimate that approximately 80 percent of these requests were related to the unauthorized attempts to access the IP PIN retrieval tool described below.

IP PIN Retrieval Tool. One aspect of the IRS's efforts to help taxpayers affected by identity theft involves the IP PIN, a unique identifier that authenticates a return filer as the legitimate taxpayer. If the IRS identifies a return as fraudulently filed, the IRS offers the legitimate taxpayer the ability to apply for an IP PIN for use when filing their next return. The IRS mails the IP PIN to the taxpayer's address of record, and the IP PIN is valid for only one filing season.

The IP PIN program began as a pilot in 2011, and since then has grown significantly. For the 2016 filing season, the IRS issued IP PINs to 2.7 million taxpayers previously identified by the IRS as victims of identity theft or participants in a pilot program. This pilot is for taxpayers living in Florida, Georgia and Washington, D.C. – three areas where there have been particularly high concentrations of stolen identity refund fraud – who can request an IP PIN regardless of whether the IRS has identified them as a victim of identity theft.

In 2015, the IRS developed an online tool that allowed taxpayers who had received an IP PIN to retrieve it if they lost or misplaced the number before filing their return. Taxpayers accessed this tool on IRS.gov by entering personal information to authenticate their identity. The retrieval tool has been used by only a small subset of all taxpayers receiving an IP PIN: this filing season, out of the 2.7 million who received an IP PIN, just 130,000, or about 5 percent, used the retrieval tool.

After discovering the problems with the Get Transcript online application, we began in July 2015 to monitor every request to recover a forgotten or lost IP PIN. In February 2016, as part of this proactive, ongoing security review, the IRS temporarily suspended this retrieval tool after detecting potentially unauthorized attempts to obtain IP PINs using the tool. Thus far, the IRS has confirmed and stopped about 5,000 false returns using a fraudulently obtained IP PIN. While our analysis is ongoing, at this time we do not believe any fraudulent refunds were issued as a result of successful unauthorized attempts to retrieve an IP PIN.

We are conducting a further review of this online tool and will strengthen its security features before bringing it back online. The IRS conducted an e-authentication risk assessment, following OMB guidelines, for the IP PIN retrieval tool, and has assigned an assurance level of 3F to this tool, so that taxpayers will have to undergo a multifactor authentication process to gain access once we bring the tool back online. Taxpayers who still need to retrieve a lost IP PIN in order to file their 2015 tax return can call the IRS, and we will mail the replacement IP PIN to the taxpayer's address of record.

Get Your Electronic Filing PIN Online Tool. Another way in which the IRS employs personal identification numbers involves the electronic signature on a tax return. When taxpayers electronically file a return, they sign their return by obtaining one of several types of PINs available through IRS.gov.

For example, the self-select PIN (SSP) method requires the taxpayer to use their prior-year adjusted gross income (AGI) or their prior-year SSP to authenticate their identity. They then select a five-digit PIN that can be any five numbers to enter as their electronic signature.

The IRS also provides an alternative to taxpayers unable to access their prior-year tax year return information for electronic signature authentication purposes. Using the Get Your Electronic Filing PIN application, taxpayers can enter identifying information and receive a temporary electronic filing PIN that can be used only for the current tax filing season. During FY 2015, taxpayers obtained approximately 25 million e-File PINs. On average, e-File PINs are used to sign about 12 million returns a year.

In January of this year, the IRS identified and halted an automated "bot" intrusion upon the Get Your Electronic Filing PIN application. In this intrusion, identity thieves employed malicious software, commonly known as "malware," to gain access to the application and generate e-File PINs for SSNs they had stolen from sources outside the IRS. Based on our review, we identified unauthorized attempts involving approximately 464,000 unique SSNs, of which 101,000 SSNs were used to successfully access an e-File PIN.

Nonetheless, our analysis of the situation found that no personal taxpayer data was compromised or disclosed by IRS systems, and no fraudulent refunds were issued. The IRS has taken steps to notify affected taxpayers by mail that their personal information was used in an attempt to access this IRS application. The IRS has also put returns filed under these SSNs through additional scrutiny to protect against future tax-related identity theft.

LOOKING TO THE FUTURE

Building an Authentication Framework

These incidents illustrate the challenges we face in developing appropriate authentication procedures for online transactions. The IRS takes protection of taxpayer data very seriously, and with that in mind, we must constantly strike a balance between citizen convenience and strong authentication and security protocols in an ever-changing cybercrime environment. The incidents also illustrate a wider truth about identity theft in general, which is that there are no perfect systems. No one, either in the public or private sector, can give an absolute guarantee that a system will never be compromised. For that reason, we continue our comprehensive efforts to update the security of our systems, protect taxpayers and their data, and investigate crimes related to stolen identity refund fraud.

We are reviewing our current e-authentication risk assessment process to ensure that the level of authentication risk for all current and future IRS online services accurately reflects the risk to the IRS and taxpayers should an authentication vulnerability occur.

We also realize that more needs to be done. A key element in our efforts to improve protections for existing online tools and new ones contemplated for the future is the development of a strong, coordinated and evolving authentication framework. This framework, once fully developed, will enable us to require multifactor authentication for all online tools and applications that warrant a high level of assurance.

To ensure proper development of our authentication framework, the IRS recently created a new position, the IRS Identity Assurance Executive. This executive will develop our Service-wide approach to authentication. In addition, we have engaged with the U.S. Digital Service (USDS), which uses the best of product design, engineering practices and technology professionals to build effective, efficient, and secure digital channels to transform the way government works for taxpayers.

We are joining forces with a team from USDS as we develop the future taxpayer digital experience and the foundational authentication standards that will enable secure digital exchanges between the IRS and taxpayers. In addition, we will leverage NIST standards to ensure that authentication processes used for all current and future online applications provide the required level of assurance for the determined level of authentication risk.

Going forward, we will continue to review and adjust our authentication protocols accordingly. The sophistication of today's cybercriminals and identity thieves requires us to continually reassess and modify these protocols.

Enhancing the Taxpayer Experience

Our efforts to detect and stop suspicious online activity and to develop a strong authentication framework are especially critical now, as the IRS builds toward the future and works to improve the online taxpayer experience for those taxpayers who prefer to communicate with us this way.

Within our tight budget constraints, the IRS has continued to analyze and develop plans for improving how the agency can fulfill its mission in the future, especially in delivering service to taxpayers.

We are looking forward to a new and improved way of doing business that involves a more robust online taxpayer experience. This is driven, in part, by business imperatives, since it costs between \$40 and \$60 to interact with a taxpayer in person, and less than \$1 to interact online. But we also need to provide the best possible taxpayer experience, in response to taxpayer expectations and demands.

While we have spent the last several years developing new tools and applications to meet these taxpayer expectations and demands, we are now at the point where we believe the taxpayer experience needs to be taken to a new level. Our goal is to increase the availability and quality of self-service interactions, which will give taxpayers the ability to take care of their tax obligations online in a fast, secure and convenient manner.

The idea is that taxpayers would have an account with the IRS where they, or their preparers, could log in securely, get all the information about their account, and interact with the IRS as needed. Most things that taxpayers need to do to fulfill their federal tax obligations could be done virtually, and there would be much less need for in-person help, either by waiting in line at an IRS assistance center or calling the IRS.

As we improve the online experience, we understand the responsibility we have to serve the needs of all taxpayers, whatever their age, income, or location. We recognize there will always be taxpayers who do not have access to the internet, or who simply prefer not to conduct their transactions with the IRS online. The IRS remains committed to providing the services these taxpayers need. We do not intend to curtail the ability of taxpayers to deal with us by phone or in person.

In building toward the future of taxpayer service, we will need to strike a delicate balance with our efforts to improve our authentication protocols described above. Authentication protocols will need to be high, but not so high as to preclude taxpayers from legitimately using the online services we provide. As criminals become increasingly sophisticated, we will need to continue recalibrating our approach to authentication to continue maintaining this balance.

The Get Transcript online application is a good example of these tradeoffs. Under the original authentication method we required for the Get Transcript

online application, we estimate that about 22 percent of legitimate taxpayers trying to access the application were unable to get through. We anticipate that under the multifactor authentication protocol to be implemented, an even higher percentage of taxpayers will be unable to use the tool. We will explain to taxpayers why these strong protections are necessary. All taxpayers will be able to order a transcript, online or by phone, and have it mailed to their address of record, if the online tool does not work for them, or if they prefer not to interact with us online.

Need for Adequate Resources and Legislative Solutions

An important consideration as we move into the future is the need for adequate resources to continue improving our efforts against identity theft and protecting our systems against cybercrime involving incidents, intrusions, and attacks. The IRS has been operating in an extremely difficult budget environment for several years, as our funding has been substantially reduced. In FY 2016, our funding level is more than \$900 million lower than it had been in FY 2010.

Despite those reductions, the IRS still devotes significant resources to cybersecurity and identity theft, even though our total needs still exceeded our available funds.

Congress provided \$290 million in additional funding for FY 2016, to improve service to taxpayers, strengthen cybersecurity and expand our ability to address identity theft. This action by lawmakers was a helpful development for the IRS and for taxpayers, and we appreciate it. Sustaining and increasing funds available for cybersecurity efforts at the IRS is critical this year and in the future. The IRS is using the new resources wisely and efficiently. This includes:

- **Cybersecurity.** We are using approximately \$95.4 million to invest in a number of critical security improvements, including more effective monitoring of data traffic and replacement of technology that supports the development, maintenance and operation of IRS applications to make processes more secure, reliable and efficient. The funding will help us to improve systems and defenses across the entire IRS, thereby helping to protect taxpayer data. We are also investing in systems to allow for enhanced network segmentation, which involves further subdividing our network, so that if any vulnerabilities occur, they would be contained to just one portion of the network.
- **Identity Theft.** We are using approximately \$16.1million to develop advanced secure access capabilities for applications such as Get Transcript, IP PIN and others. This will also fund advanced analytics and detection of anomalies in returns filed. In addition, this investment will allow the IRS to partner with private industry and state tax agencies

through the Security Summit to, for the first time, share information systemically about suspicious activity in the tax system.

- **Taxpayer Service.** We are using approximately \$178.4 million provided in the additional \$290 million to add about 1,000 extra temporary employees to help improve our service on our toll-free phone lines. As a result, we are already seeing service improvements. So far this filing season, the telephone level of service (LOS) is nearly 75 percent, and the average for the entire filing season will probably be above 70 percent, which is a vast improvement over last year. The IRS has prioritized LOS during filing season, and was operating at historically low levels up until the new appropriations were provided in December. In fact, we expect LOS for the full year to be about 47 percent. The 2017 Budget provides LOS above 70 percent for the full year with an investment of \$150 million above current levels, and by supplementing with user fees.

The FY 2017 President's Budget sustains and bolsters funding for these important programs. This includes \$90 million in additional funding to help prevent identity theft and refund fraud and to reduce improper payments. This funding will increase the capacity of our most important programs discussed above, including external leads and criminal investigations. New funds will allow the IRS to close almost 100,000 additional identity theft cases per year by helping victimized taxpayers who have engaged the IRS for assistance. The number of identity theft cases has grown from 188,000 in FY 2010 to 730,000 in FY 2014, and current resources can only close about 409,000 per year.

The FY 2017 President's Budget also requests cybersecurity funds provided through a Department wide Cybersecurity Enhancement account, which will bolster Treasury's overall cybersecurity posture. Of the nearly \$110 million requested in the account, \$54.7 million will directly support IRS cybersecurity efforts by securing data, improving continuous monitoring, and other initiatives. An additional \$7.4 million will be used to continue development and implementation of electronic authentication systems currently being developed for the Get Transcript online application for our expanding set of digital services.

While adequate funding is critical to improving our cybersecurity efforts, Congress also provides important support to the IRS by passing legislative proposals that improve tax administration. An excellent example is the enactment last December of the requirement for companies to file Form W-2s and certain other information returns earlier in the year than now. Having W-2s earlier will make it easier for the IRS to verify the legitimacy of tax returns at the point of filing and to spot fraudulent returns.

Although the new law is not effective until the 2017 filing season, some employers that issue large volumes of W-2s agreed this year to voluntarily file them earlier in the year, so the benefit of the change is already beginning to be

felt. This year we received early submissions of about 26 million W-2s, most of which came in by the end of January. The IRS is using this data in our program to verify claims of wages and withholding on individual income tax returns. We expect this to assist in the quicker release of refunds for those returns we are able to verify.

We have asked Congress for other changes to enhance tax administration and help us in our efforts to improve cybersecurity. An important proposal is the reauthorization of so-called streamlined critical pay authority, originally enacted in 1998, to assist the IRS in bringing in individuals from the private sector with the skills and expertise needed in certain highly specialized areas, including IT, international tax and analytics support. This authority, which ran effectively for many years, expired at the end of FY 2013 and was not renewed.

The loss of streamlined critical pay authority has created major challenges to our ability to retain employees with the necessary high-caliber expertise in the areas mentioned above. In fact, out of the many expert leaders and IT executives hired under critical pay authority, there are only 10 IT experts remaining at the IRS, and we anticipate there will be no staff left under critical pay authority by this time next year. The President's FY 2017 Budget proposes reinstating this authority, and I urge the Congress to approve this proposal.

Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittee, this concludes my statement. I would be happy to take your questions.



Commissioner John Koskinen



John Koskinen is the 48th IRS Commissioner. As Commissioner, he presides over the nation's tax system, which collects approximately \$3.1 trillion in tax revenue each year. This revenue funds most government operations and public services. Mr. Koskinen manages an agency of about 90,000 employees and a budget of approximately \$10.9 billion.

In his role leading the IRS, Mr. Koskinen is working to ensure that the agency maintains an appropriate balance between taxpayer service and tax enforcement and administers the tax code with fairness and integrity.

Prior to his appointment, Mr. Koskinen served as the non-executive chairman of Freddie Mac from 2008 to 2012 and its acting chief executive officer in 2009. Previously, Mr. Koskinen served as President of the U.S. Soccer Foundation, Deputy Mayor and City Administrator of Washington D.C., Assistant to the President and Chair of the President's Council on Year 2000 Conversion and Deputy Director for Management at the Office of Management and Budget. Mr. Koskinen also spent 21 years in the private sector in various leadership positions with the Palmieri Company, including President and Chief Executive Officer, helping to turn around large, troubled organizations. He began his career clerking for Chief Judge David L. Bazelon of the DC Circuit Court of Appeals in 1985, practiced law with the firm of Gibson, Dunn and Crutcher and served as Assistant to the Deputy Executive Director of the National Advisory Commission on Civil Disorders, also known as the Kerner Commission. Mr. Koskinen also served as Legislative Assistant to New York Mayor John Lindsay and Administrative Assistant to Sen. Abraham Ribicoff of Connecticut.

Mr. Koskinen holds a Law Degree from Yale University School of Law and a Bachelor's Degree from Duke University. He also studied International Law for one year in Cambridge, England. He and his wife Patricia have two grown children and live in Washington, DC.

Page Last Reviewed or Updated: 02-Dec-2015

Chairwoman COMSTOCK. Mr. George.

**TESTIMONY OF THE HONORABLE J. RUSSELL GEORGE,
INSPECTOR GENERAL,
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION**

Mr. GEORGE. Thank you, Chairwoman Comstock, Ranking Member Lipinski, Chairman Smith, and members of the Subcommittee. Thank you for the opportunity to testify on the IRS's actions to protect taxpayers' personal information.

For the last six years, we have identified the security of taxpayer data as the most serious management challenge confronting the IRS. Based on our work on information technology security, TIGTA has identified a number of areas in which the IRS could do better to protect taxpayer data.

The IRS has been moving towards providing more services through the internet referred to as online services. Web applications that provide online services must be set up in a secure manner. Even without breaching the security of the application or hardware, hackers can pose as legitimate users in order to make it through the authentication process and obtain sensitive data.

Recent security incidents, has been noted during the outset of this hearing, that involved two of the IRS's online service applications, are prime examples of what can go wrong when security is inadequate. While the IRS had established processes and procedures to authenticate individuals requesting online access to IRS services, they did not comply with government standards. For example, the processes that the IRS used to authenticate users of the "Get Transcript" and Identity Protection Personal Identification Number applications required only single-factor authentication. However, government standards require multifactor authentication for such high-risk applications. Of further concern, the authentication framework used for these applications did not comply with government standards for single-factor authentication.

In August 2015, the IRS reported that unauthorized users had been successful in obtaining tax information on the "Get Transcript" application for an estimated 334,000 taxpayer accounts, as you noted, Madam Chairwoman. To prevent further unauthorized access, the IRS removed the application from its website. TIGTA's subsequent review of the "Get Transcript" breach identified additional suspicious accesses to taxpayers' accounts that the IRS had not identified. Based on TIGTA's analysis, the IRS reported on February 26th of this year that potentially unauthorized users had been successful in obtaining access to an additional 390,000 taxpayer accounts, again, as has been noted.

We also reported in November 2015 that the IRS did not complete the required authentication risk assessment for its Identify Protection PIN application and recommended that the IRS not reactivate this application for the 2016 filing season. However, the IRS reactivated the application on January 19th of this year. We issued a second recommendation to the IRS on February 24th advising it to remove the Identity Protection PIN application from its public website. On March 7th, the IRS reported that it was temporarily suspending use of the Identity Protection PIN application as part of an ongoing security review.

The IRS does not anticipate having the technology in place for either the “Get Transcript” or Identity Protection PIN application to provide multifactor authentication capability before the summer of 2016. In addition, TIGTA’s assessment of the IRS’s compliance with information security standards and guidelines found that while the IRS information security program generally complied with the requirements of FISMA—the Federal Information Security Modernization Act—there were three security program areas which did not, and they are continuous monitoring management, configuration management, and identity and access management. Until the IRS takes steps to improve these security program deficiencies and fully implement all security program areas in compliance with requirements, taxpayer data will remain vulnerable to inappropriate and undetected use, modification for disclosure.

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

[The prepared statement of Mr. George follows:]

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

"Protection of Taxpayers' Personal Information"



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

April 14, 2016

Washington, D.C.

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

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

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

The Treasury Inspector General for Tax Administration (TIGTA) is statutorily mandated to provide independent audit and investigative services necessary to improve the economy, efficiency, and effectiveness of IRS operations, including the IRS Chief Counsel. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA's role is critical in that we provide the American taxpayer with assurance that the approximately 86,000 IRS employees¹ who collected over \$3.3 trillion in tax revenue, processed over 244 million tax returns, and issued more than \$400 billion in tax refunds during Fiscal Year (FY) 2015,² have done so in an effective and efficient manner while minimizing the risks of waste, fraud, and abuse.

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

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

¹ Total IRS staffing as of October 3, 2015. Included in the total are approximately 15,400 seasonal and part-time employees.

² IRS, *Management's Discussion & Analysis, Fiscal Year 2015*.

employees and facilities, and other attempts to impede or otherwise interfere with the IRS's ability to collect taxes. Specifically, the Office of Investigations investigates misconduct by IRS employees which manifests itself in many ways, including unauthorized access to taxpayer information and the use of the information for the purposes of identity theft; extortion; theft of government property; taxpayer abuses; false statements; and other financial fraud. The Office of Investigations is statutorily charged to investigate threats made against the IRS's employees, facilities and data. We are committed to ensuring the safety of IRS employees and the taxpayers who conduct business at the approximately 550 offices³ in the United States and abroad.

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

Cybersecurity threats against the Federal Government continue to grow. Since 2011, my office has identified the security of taxpayer data as the most serious management and performance challenge confronting the IRS. According to the Department of Homeland Security's U.S. Computer Emergency Readiness Team, Federal agencies reported 77,183 cyberattacks in FY 2015, an increase of more than 10 percent from FY 2014.⁴

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

³ IRS, *Management's Discussion & Analysis, Fiscal Year 2015*.

⁴ Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act* (Mar. 2016).

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

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

IRS AUTHENTICATION PROCESSES NEED IMPROVEMENT

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

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

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

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

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

The existence of differing levels of authentication assurance among the various access methods increases the risk of unscrupulous individuals accessing and obtaining personal taxpayer information and/or defrauding the tax system. Unscrupulous individuals can identify the weakest points of authentication and exploit them to inappropriately gain access to tax account information. For example, on May 26, 2015, the IRS announced that unauthorized access attempts were made by individuals using taxpayer-specific data to gain access to tax information⁶ through its Get Transcript application. According to the IRS, one or more individuals succeeded in clearing the IRS's authentication process that required knowledge of information about the taxpayer, including Social Security information, date of birth, tax filing status, and street address. To prevent further unauthorized accesses, the IRS removed the application from its website.

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

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

⁶ The tax information that can be accessed on the Get Transcript application can include the current and three prior years of tax returns, nine years of tax account information, and wage and income information.

⁷ OMB, M-04-04, *E-Authentication for Federal Agencies* (Dec. 2003).

⁸ NIST, NIST SP-800-63-2, *Electronic Authentication Guideline* (Aug. 2013).

Table 1 - Levels of Electronic Assurance

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

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

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

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

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

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

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

In August 2015, the IRS indicated that unauthorized users had been successful¹⁰ in obtaining information on the Get Transcript application for an estimated 334,000 taxpayer accounts. TIGTA's current review¹¹ of the Get Transcript breach identified additional suspicious accesses to taxpayers' accounts that the IRS had not identified. Based on TIGTA's analysis of Get Transcript access logs, the IRS

¹⁰ A successful access is one in which the unauthorized users successfully answered identity proofing and knowledge-based authentication questions required to gain access to taxpayer account information.

¹¹ TIGTA, Audit No. 201540027, *Evaluation of Assistance Provided to Victims of the Get Transcript Data Breach*, report planned for May 2016.

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

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

We are currently evaluating the appropriateness of the IRS's response to the Get Transcript incident and the IRS's proposed solutions to address the authentication weakness that allowed the incident to occur.¹² During our audit work, we have learned that the IRS is working with the U.S. Digital Service¹³ on its new e-authentication and authorization policies and procedures. In addition, TIGTA is participating in a multi-agency investigation into this matter, and we have provided the IRS with some of our investigative observations to date in order to help them secure the e-authentication environment in the future.

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

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

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

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

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

DATA SECURITY REMAINS A TOP CONCERN OF TIGTA

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

During our most recent Federal Information Security Modernization Act¹⁴ evaluation of the IRS's information security programs and practices,¹⁵ we found three security program areas, *i.e.*, Continuous Monitoring Management, Identity and Access Management, and Configuration Management, that did not meet the level of

¹⁴ Pub. L. No. 113-283, 128 Stat. 3073 (2014). This bill amended chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

¹⁵ TIGTA, Ref. No. 2015-20-092, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2015* (Sept. 2015).

performance specified by the Department of Homeland Security.¹⁶

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

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

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

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

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

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

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

TIGTA also found that many interconnections¹⁹ in use at the IRS do not have proper authorization or are not covered by security agreements. Although the IRS has established an office to provide oversight and guidance for the development of security agreements, that office is not responsible for managing or monitoring agreements for all external interconnections in use in the IRS environment. TIGTA believes the lack of a centralized inventory and of an enterprise-level approach to ensure that all external interconnections are monitored have contributed to interconnections that are active but lack proper approvals and assurances necessary to meet current security requirements.²⁰

In addition, TIGTA reported²¹ that the IRS was unable to upgrade all of its workstations with the most current Windows® operating system.²² Because of their importance, operating systems must be updated on a regular basis to patch security vulnerabilities and, if necessary, upgraded completely in order to fix crucial weaknesses or to address new threats to their functionality. TIGTA found that the IRS did not follow established policies with respect to project management and provided inadequate

¹⁷ TIGTA, Ref. No. 2012-20-019, *The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed* (Mar. 2012).

¹⁸ TIGTA, Audit No. 201620003, *Effectiveness of the Computer Security Incident Response Center*, report planned for September 2016.

¹⁹ The National Institute of Standards and Technology defines a system interconnection as the direct connection of two or more information technology systems for the purpose of sharing data and other information resources.

²⁰ TIGTA, Ref. No. 2015-20-087, *Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured* (Sept. 2015).

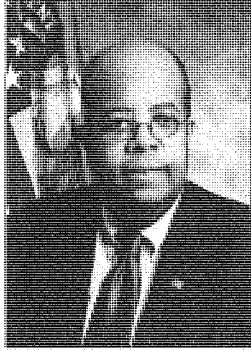
²¹ TIGTA, Ref. No. 2015-20-073, *Inadequate Early Oversight Led to Windows Upgrade Project Delays* (Sept. 2015).

²² The software that communicates with computer hardware to allocate memory, process tasks, access disks and peripherals, and serves as the user interface.

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

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

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



J. Russell George

Treasury Inspector General for Tax Administration

Following his nomination by President George W. Bush, the United States Senate confirmed J. Russell George in November 2004, as the Treasury Inspector General for Tax Administration. Prior to assuming this role, Mr. George served as the Inspector General of the Corporation for National and Community Service, having been nominated to that position by President Bush and confirmed by the Senate

in 2002.

A native of New York City, where he attended public schools, including Brooklyn Technical High School, Mr. George received his Bachelor of Arts degree from Howard University in Washington, DC, and his Doctorate of Jurisprudence from Harvard University's School of Law in Cambridge, MA. After receiving his law degree, he returned to New York and served as a prosecutor in the Queens County District Attorney's Office.

Following his work as a prosecutor, Mr. George joined the Counsel's Office in the White House Office of Management and Budget, where he was Assistant General Counsel. In that capacity, he provided legal guidance on issues concerning presidential and executive branch authority. He was next invited to join the White House Staff as the Associate Director for Policy in the Office of National Service. It was there that he implemented the legislation establishing the Commission for National and Community Service, the precursor to the Corporation for National and Community Service. He then returned to New York and practiced law at Kramer, Levin, Naftalis, Nessen, Kamin & Frankel.

In 1995, Mr. George returned to Washington and joined the staff of the Committee on Government Reform and Oversight and served as the Staff Director and Chief Counsel of the Government Management, Information and Technology subcommittee (later renamed the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations), chaired by Representative Stephen Horn. There he directed a staff that conducted over 200 hearings on legislative and oversight issues pertaining to Federal Government management practices, including procurement policies, the disposition of government-controlled information, the performance of chief financial officers and inspectors general, and the Government's use of technology. He continued in that position until his appointment by President Bush in 2002.

Mr. George also served as a member of the Integrity Committee of the Council of Inspectors General for Integrity and Efficiency (CIGIE). CIGIE is an independent entity within the executive branch, statutorily established by the Inspector General Act, as amended, to address integrity, economy, and effectiveness issues that transcend individual Government agencies and to increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General. The CIGIE Integrity Committee serves as an independent review and investigative mechanism for allegations of wrongdoing brought against Inspectors General.

Chairwoman COMSTOCK. Thank you.

**TESTIMONY OF MR. GREGORY WILSHUSEN, DIRECTOR,
INFORMATION SECURITY ISSUES,
U.S. GOVERNMENT ACCOUNTABILITY OFFICE**

Mr. WILSHUSEN. Chairwoman Comstock, Ranking Member Lipinski, Chairman Smith, and Members of the Subcommittee, thank you for the opportunity to testify on IRS's Information Security program.

As part of GAO's annual audit of IRS's financial statements, we examined the information security controls over the Service's financial and tax processing systems. As we reported in March, IRS has implemented numerous protections over these systems but weaknesses remain in controls that are intended to prevent, detect and limit unauthorized access to systems and the information they contain.

IRS had developed controls for identifying and authenticating the identity of users and servers. However, they were inconsistently implemented. For example, the agency used easily guessed passwords on servers supporting several systems including those relating to procurements, automated file transfers, management of taxpayer accounts, and processing of electronic tax payment information. In addition, users were granted excessive access permissions on 11 of 14 systems we reviewed including on one system which allowed users to access or change tax payment-related data.

IRS policies require use of encryption, and the agency continued to expand its use. However, sensitive administrative credentials were not encrypted on key systems that we reviewed. Software patches were often not installed in a timely manner on several systems including at least one critical patch that has been available since August 2012. To its credit, IRS had established contingency plans for the systems we review, which help to ensure that critical operations can continue when unexpected events occur. Nevertheless, the control weaknesses we identified were caused in part by IRS's inconsistent execution of its information security program. Including the 45 new recommendations we made in March, IRS has yet to implement 94 of our recommendations. Implementing these recommendations will assist IRS in bolstering its information security and protection over taxpayer information. Until it does so, taxpayer and financial data will continue to be exposed to unnecessary risk.

The importance of protecting taxpayer information is further highlighted by the recent incidents involving the "Get Transcript" online service and the billions of dollars that have been lost to identity theft refund fraud. This type of fraud occurs when a criminal obtains personally identifiable information of a legitimate taxpayer and uses it to file a fraudulent return seeking a refund. Because of its continuing significance, we added IRS's efforts to combat identity theft refund fraud to our high-risk area on the enforcement of tax laws. IRS has acted to address this problem but additional actions are needed.

In January 2015, we reported that its tools for authenticating the identity of taxpayers using e-file had limitations and recommended

that IRS assess the risks, costs and benefits of its authentication options.

To assist and guide federal efforts, OMB—the Office of Management and Budget—and the National Institute of Standards and Technology play a key role in developing information security policies, standards, and guidelines for federal agencies. Among other things, OMB and NIST have developed guidance for agencies implementing e-authentication protocols. OMB is responsible for overseeing and holding agencies accountable for complying with information security requirements such as those provided in the Federal Information Security Modernization Act of 2014.

In summary, IRS has made progress implementing security protections over its tax-processing and financial systems. However, it needs to do more to adequately safeguard taxpayer data. Until IRS fully implements all of our recommendations to mitigate deficiencies in access and other controls, to consistently implement elements of its Information Security program, and to assess the risks, costs and benefits of its authentication options, taxpayer information will remain at unnecessary risk.

Chairwoman Comstock, Ranking Member Lipinski, Chairman Smith, this concludes my statement. I'd be happy to answer your questions.

[The prepared statement of Mr. Wilshusen follows:]



United States Government Accountability Office

Testimony

Before the Subcommittee on Research and
Technology, Committee on Science, Space, and
Technology, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, April 14, 2016

INFORMATION SECURITY

IRS Needs to Further Enhance Controls over Taxpayer and Financial Data

Statement of Gregory C. Wilshusen
Director, Information Security Issues

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO Highlights

Highlights of GAO-16-590T, a testimony before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives

Why GAO Did This Study

In collecting taxes, processing returns, and providing taxpayer service, IRS relies extensively on computerized information systems. Accordingly, it is critical that sensitive taxpayer and other data are protected. Recent data breaches at IRS highlight the vulnerability of taxpayer information. In addition, identity theft refund fraud is an evolving threat that occurs when a thief files a fraudulent tax return using a legitimate taxpayer's identity and claims a refund.

Since 1997, GAO has designated federal information security as a government-wide high-risk area, and in 2015 it expanded this area to include the protection of personally identifiable information. GAO also added identity theft refund fraud to its high-risk area on the enforcement of tax laws.

This statement discusses (1) IRS's information security controls over tax processing and financial systems and (2) roles that federal agencies with government-wide information security responsibilities play in providing guidance and oversight to agencies. This statement is based on previously published GAO work and a review of federal guidance.

What GAO Recommends

In addition to 49 prior recommendations that had not been implemented, GAO made 45 new recommendations to IRS in March 2016 to further improve its information security controls and program. GAO also recommended that IRS assess costs, benefits, and risks of taxpayer authentication options.

View GAO-16-590T. For more information, contact Gregory C. Wilshusen at (202) 512-5244 or wilshusen@gao.gov or James R. McTigue, Jr. at (202) 512-9110 or mctiguej@gao.gov.

April 14, 2016

INFORMATION SECURITY

IRS Needs to Further Enhance Controls over Taxpayer and Financial Data

What GAO Found

In March 2016 GAO reported that the Internal Revenue Service (IRS) had instituted numerous controls over key financial and tax processing systems; however, it had not always effectively implemented safeguards intended to properly restrict access to systems and information. In particular, while IRS had improved some of its access controls, weaknesses remained with identifying and authenticating users, authorizing users' level of rights and privileges, encrypting sensitive data, auditing and monitoring network activity, and physically securing its computing resources. These weaknesses were due in part to IRS's inconsistent implementation of its agency-wide security program, including not fully implementing GAO recommendations. The table below shows the status of prior and new GAO recommendations as of the end of its fiscal year (FY) 2015 audit of IRS's information security. GAO concluded that these weaknesses collectively constituted a significant deficiency for the purposes of financial reporting for fiscal year 2015. Until they are effectively mitigated, taxpayer and financial data will continue to be exposed to unnecessary risk.

Status of GAO Information Security Recommendations to IRS as of March 2016				
Information security control area	Prior GAO recommendations open at the start of FY 2015 audit	Recommendations closed during FY 2015 audit	New recommendations	Outstanding recommendations at end of FY 2015 audit
Information security program	12	(3)	2	11
Access controls	34	(11)	38	61
Other controls	24	(7)	5	22
Totals	70	(21)	45	94

Source: GAO analysis of IRS data. | GAO-16-590T

The importance of protecting taxpayer information is further highlighted by the billions of dollars that have been lost to identity theft refund fraud, which continues to be an evolving threat. While IRS has taken steps to address this issue, as GAO reported in January 2015 it has yet to assess the costs, benefits, and risks of methods for improving the authentication of taxpayers' identity.

The Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) provide government-wide guidance and oversight for federal information security. These agencies have taken a number of actions to carry out these responsibilities. For example:

- OMB has prescribed security policies, including direction on ensuring that online services provided by agencies are secure and protect privacy.
- NIST has developed standards and guidelines for implementing security controls, including those for authenticating users during online transactions.
- DHS has issued a directive requiring departments and agencies to mitigate critical vulnerabilities on their Internet-facing systems. It also assists agencies in monitoring their networks for malicious traffic.

Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's timely hearing on information security at the Internal Revenue Service (IRS). As taxpayers file their returns for 2015, it is especially important that IRS ensure that adequate protections are in place to secure the sensitive information entrusted to the agency by members of the public.

The federal government faces an evolving array of cyber-based threats to its systems and data. Reported incidents and data breaches at federal agencies, including IRS, have affected millions of people through the compromise of sensitive personal information and underscore the continuing and urgent need for effective information security. We initially designated federal information security as a government-wide high-risk area in 1997, and in 2003 we expanded this area to include computerized systems supporting the nation's critical infrastructure. In 2015 we added the protection of personally identifiable information (PII)¹ that is collected, maintained, and shared by both federal and nonfederal entities.²

In carrying out its mission to collect taxes, process tax returns, and enforce U.S. tax laws, IRS relies extensively on computerized systems and on information security controls to protect the confidentiality, integrity, and availability of sensitive personal and financial information for each U.S. taxpayer.

As requested, my statement today will discuss (1) information security controls over tax processing and financial systems at IRS and (2) roles that federal agencies with government-wide information security responsibilities play in providing guidance and oversight to executive branch agencies. In preparing this statement, we relied on previously published work on IRS and government-wide information security. We also reviewed relevant federal laws and information security-related guidance issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). The GAO reports cited in this statement each contain a detailed description of the scope of

¹PII is information about an individual, including information that can be used to distinguish or trace their identity, such as name, Social Security number, mother's maiden name, or biometric records, as well as any other personal information that is linked or linkable to an individual.

²GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

the work on which they are based and the methodologies used to carry it out.

All the work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As technology has advanced, the federal government has become increasingly dependent on computerized information systems to carry out operations and process, maintain, and report essential information. Federal agencies rely on such systems to process, maintain, and report large volumes of sensitive data, such as personal information.

Ineffective protection of these systems and information can impair delivery of vital services and result in

- loss or theft of computer resources, assets, and funds;
- inappropriate access to and disclosure, modification, or destruction of sensitive information, such as PII;
- undermining of agency missions due to embarrassing incidents that erode the public's confidence in government;
- damage to networks and equipment; and
- high costs for remediation.

Recognizing the importance of these issues, federal law includes requirements intended to improve the protection of government information and systems. These laws include the Federal Information Security Modernization Act (FISMA) of 2014, which among other things, requires the head of each agency to provide information security protections commensurate with the risk and magnitude of harm resulting

from unauthorized access, use, disclosure, disruption, modification, or destruction of the agency's information or information systems.³

More specifically, federal agencies are to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the operations of the agency, including those provided or managed by another agency, a contractor, or other organization on behalf of the agency. In addition, the head of each agency is responsible for, among other things, ensuring that senior agency officials carry out their information security responsibilities and that all personnel are held accountable for complying with the agency-wide information security program.

The act also assigned OMB and the Department of Homeland Security (DHS) oversight responsibilities to assist agencies in effectively implementing information security protections. In addition, NIST is responsible for developing standards and guidelines that include minimum information security requirements.

IRS Relies on Information Technology Systems to Carry out Its Role as Tax Collector for the United States

IRS's mission is to provide America's taxpayers top-quality service by helping them to understand and meet their tax responsibilities and to enforce the law with integrity and fairness to all. In carrying out its mission, IRS relies extensively on computerized information systems, which it must effectively secure to protect sensitive financial and taxpayer data for the collection of taxes, processing of tax returns, and enforcement of federal tax laws.

During fiscal year 2015, IRS collected more than \$3.3 trillion; processed more than 243 million tax returns and other forms; and issued more than \$403 billion in tax refunds.

IRS employs about 90,000 people in its Washington, D.C., headquarters and at more than 550 offices in all 50 states, U.S. territories, and some

³The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014)) partially superseded the Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this statement, "FISMA" refers to the new requirements in FISMA 2014, FISMA 2002 requirements relevant here that were incorporated and continued in FISMA 2014, and other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

U.S. embassies and consulates. To manage its data and information, the agency operates two enterprise computing centers. It also collects and maintains a significant amount of personal and financial information on each U.S. taxpayer. Protecting this sensitive information is essential to protecting taxpayers' privacy and preventing financial loss and damages that could result from identity theft and other financial crimes. Further, the size and complexity of the IRS add unique operational challenges.

The Commissioner of Internal Revenue has overall responsibility for ensuring the confidentiality, integrity, and availability of the information and systems that support the agency and its operations. Within IRS, the senior agency official responsible for information security is the Associate CIO, who heads the IRS Information Technology Cybersecurity organization.

Cyber Threats Facing Federal Systems Continue to Evolve

Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused by natural disasters, defective computer or network equipment, software coding errors, and the actions of careless or poorly trained employees. Intentional threats include targeted and untargeted attacks from criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists. These adversaries vary in terms of their capabilities, willingness to act, and motives.

These threat sources make use of various techniques—or exploits—that may adversely affect federal information, computers, software, networks, and operations. These exploits are carried out through various conduits, including websites, e-mails, wireless and cellular communications, Internet protocols, portable media, and social media. Further, adversaries can leverage common computer software programs as a means by which to deliver a threat by embedding exploits within software files that can be activated when a user opens a file within its corresponding program.

The number of information security incidents affecting systems supporting the federal government is increasing. Specifically, the number of incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) increased from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent. This upward trend continues. According to OMB, agencies reported 77,183 incidents in fiscal year 2015. Similarly, the number of incidents involving PII reported by federal agencies has more than doubled in recent years, from 10,481 in 2009 to 27,624 in 2014.

Moreover, for fiscal year 2015, OMB reported that federal agencies spent about \$13.1 billion on cybersecurity,⁴ and agencies budgeted about \$14 billion for cybersecurity for fiscal year 2016.⁵ This amount may increase significantly, as the president's fiscal year 2017 budget proposes investing over \$19 billion in resources for cybersecurity.

Cyber incidents can adversely affect national security, damage public health and safety, and compromise sensitive information. Regarding IRS specifically, two recent incidents illustrate the impact on taxpayer and other sensitive information:

- In June 2015, the Commissioner of the IRS testified that unauthorized third parties had gained access to taxpayer information from its Get Transcript application.⁶ According to officials, criminals used taxpayer-specific data acquired from non-agency sources to gain unauthorized access to information on approximately 100,000 tax accounts. These data included Social Security information, dates of birth, and street addresses. In an August 2015 update, IRS reported this number to be about 114,000, and reported that an additional 220,000 accounts had been inappropriately accessed. In a February 2016 update, the agency reported that an additional 390,000 accounts had been accessed. Thus, about 724,000 accounts were reportedly affected. The online Get Transcript service has been unavailable since May 2015.
- In March 2016, IRS stated that as part of its ongoing security review, it had temporarily suspended the Identity Protection Personal Identification Number (IP PIN) service on IRS.gov. The IP PIN is a single-use identification number provided to taxpayers who are victims

⁴OMB, *Annual Report to Congress: Federal Information Security Modernization Act*, (Washington, D.C.: Mar. 18, 2016).

⁵OMB, *Middle Class Economics: Cybersecurity*, The President's Budget Fiscal Year 2016 (Washington, D.C.: Feb. 2, 2015).

⁶This application provides users, via the IRS website, the ability to view, print, and download tax account, tax return, and record of account transcripts; wage and income documents; and proof of non-filing transcripts.

of identity theft (IDT) to help prevent future IDT refund fraud.⁷ The service on IRS's website allowed taxpayers to retrieve their IP PINs online by passing IRS's authentication checks. These checks confirm taxpayer identity by asking for personal, financial, and tax-related information. The IRS stated that it was conducting further review of the IP PIN service and is looking at further strengthening the security features. As of April 7, the online service was still suspended.

Although IRS Has Made Improvements, Information Security Weaknesses Continue to Place Taxpayer and Financial Data at Risk

As we reported in March 2016, IRS has implemented numerous protections over key financial and tax processing systems; however, it had not always effectively implemented access and other controls, including elements of its information security program.⁸

Access controls are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. They include identification and authentication, authorization, cryptography, audit and monitoring, and physical security, among others. In our most recent review we determined that IRS had improved access controls, but some weaknesses remain.

- **Identifying and authenticating users**—such as through user account-password combinations—provides the basis for establishing accountability and controlling access to a system. IRS established policies for identification and authentication, including requiring

⁷In January 2014, IRS offered a limited IP PIN pilot program to eligible taxpayers in Florida, Georgia, and the District of Columbia. Taxpayers must confirm their identities with IRS to receive an IP PIN. IP PINs help prevent identity theft refund fraud (discussed later in this statement) because, once issued, the IP PIN must accompany their electronically filed tax return or else IRS will reject the return. If a paper return has a missing or incorrect IP PIN, IRS delays processing the return while the agency determines if it was filed by the legitimate taxpayer.

⁸GAO, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, GAO-16-398 (Washington, D.C.: Mar. 28, 2016).

multifactor authentication⁹ for local and network access accounts and establishing password complexity and expiration requirements. It also improved identification and authentication controls by, for example, expanding the use of an automated mechanism to centrally manage, apply, and verify password requirements. However, weaknesses in identification and authentication controls remained. For example, the agency used easily guessable passwords on servers supporting key systems. In addition, while IRS continued to expand the use of two-factor access to its network, the Treasury Inspector General for Tax Administration reported that IRS had not fully implemented unique user identification and authentication or remote electronic authentication that complies with federal requirements.¹⁰

- **Authorization controls** limit what actions users are able to perform after being allowed into a system and should be based on the concept of "least privilege," granting users the least amount of rights and privileges necessary to perform their duties. While IRS established policies for authorizing access to its systems, it continued to permit excessive access in some cases. For example, users were granted rights and permissions in excess of what they needed to perform their duties, including for an application used to process electronic tax payment information and a database on a human resources system.
- **Cryptography controls** protect sensitive data and computer programs by rendering data unintelligible to unauthorized users and protecting the integrity of transmitted or stored data. IRS policies require the use of encryption, and the agency continued to expand its use of encryption to protect sensitive data. However, key systems we reviewed had not been configured to encrypt sensitive user authentication data.

⁹Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric).

¹⁰Treasury Inspector General for Tax Administration, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2015*, 2015-20-092 (Sept. 25, 2015). Homeland Security Presidential Directive 12, issued in August 2004, directed the establishment of a mandatory government-wide standard for secure and reliable forms of identification for federal employees and contractor personnel who access government-controlled facilities and information systems.

-
- **Audit and monitoring** is the regular collection, review, and analysis of events on systems and networks in order to detect, respond to, and investigate unusual activity. IRS established policies and procedures for auditing and monitoring its systems and continued to enhance its capability by, for example, implementing an automated mechanism to log user activity on its access request and approval system. But it had not established logging for two key applications used to support the transfer of financial data and access and manage taxpayer accounts; nor was the agency consistently maintaining key system and application audit plans.
 - **Physical security controls**, such as physical access cards, limit access to an organization's overall facility and areas housing sensitive IT components. IRS established policies for physically protecting its computer resources and physical security controls at its enterprise computer centers, such as a dedicated guard force at each of its computer centers. However, the agency had yet to address weaknesses in its review of access lists for both employees and visitors to sensitive areas.

IRS also had weaknesses in configuration management controls, which are intended to prevent unauthorized changes to information system resources (e.g., software and hardware) and provide assurance that systems are configured and operating securely. Specifically, while IRS developed policies for managing the configuration of its IT systems and improved some configuration management controls, it did not, for example, ensure security patch updates were applied in a timely manner to databases supporting two key systems we reviewed, including a patch that had been available since August 2012.

To its credit, IRS had established contingency plans for the systems we reviewed, which help ensure that when unexpected events occur critical operations can continue without interruption or can be promptly resumed, and that information resources are protected. Specifically, IRS had established policies for developing contingency plans for its information systems and for testing those plans, as well as for implementing and enforcing backup procedures. Moreover, the agency had documented and tested contingency plans for its systems and improved continuity of operations controls for several systems.

Nevertheless, the control weaknesses can be attributed in part to IRS's inconsistent implementation of elements of its agency-wide information security program. The agency established a comprehensive framework for its program, including assessing risk for its systems, developing system security plans, and providing employees with security awareness

and specialized training. However, IRS had not updated key mainframe policies and procedures to address issues such as comprehensively auditing and monitoring access.

In addition, the agency had not fully mitigated previously identified deficiencies or ensured that its corrective actions were effective. During our most recent review, IRS told us it had completed corrective actions for 28 of our prior recommendations; however, we determined that 9 of these had not been effectively implemented.

The collective effect of the deficiencies in information security from prior years that continued to exist in fiscal year 2015, along with the new deficiencies we identified, are serious enough to merit the attention of those charged with governance of IRS and therefore represented a significant deficiency in IRS's internal control over financial reporting systems as of September 30, 2015.¹¹

Implementing GAO Recommendations Can Help IRS Better Protect Sensitive Taxpayer and Financial Data

To assist IRS in fully implementing its agency-wide information security program, we made two new recommendations to more effectively implement security-related policies and plans. In addition, to assist IRS in strengthening security controls over the financial and tax processing systems we reviewed, we made 43 technical recommendations in a separate report with limited distribution to address 26 new weaknesses in access controls and configuration management.¹²

Implementing these recommendations—in addition to the 49 outstanding recommendations from previous audits—will help IRS improve its controls for identifying and authenticating users, limiting users' access to the minimum necessary to perform their job-related functions, protecting

¹¹A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit the attention of those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

¹²GAO, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, GAO-16-397SU (Washington, D.C.: Mar. 28, 2016).

sensitive data when they are stored or in transit, auditing and monitoring system activities, and physically securing its IT facilities and resources.

Table 1 below provides the number of our prior recommendations to IRS that were not implemented at the beginning of our fiscal year 2015 audit, how many were resolved by the end of the audit, new recommendations, and the total number of outstanding recommendations at the conclusion of the audit.

Table 1: Status of GAO's Information Security Recommendations at the Conclusion of Fiscal Year 2015 Audit

Control area	Prior recommendations not implemented at the beginning of fiscal year 2015 audit	Recommendations implemented or considered no longer relevant at the end of fiscal year 2015 audit	Prior recommendations not fully implemented at the end of fiscal year 2015 audit	New recommendations made during fiscal year 2015 audit	Total outstanding recommendations at the conclusion of fiscal year 2015 audit
Information security program	12	(3)	9	2	11
Access controls					
Identification and authentication	6	(1)	5	9	14
Authorization	10	(4)	6	12	18
Cryptography	8	(3)	5	14	19
Audit and monitoring	6	(1)	5	3	8
Physical Security	4	(2)	2	0	2
Other security controls					
Configuration management	21	(5)	16	5	21
Segregation of duties	1	(0)	1	0	1
Contingency planning	2	(2)	0	0	0
Total:	70	(21)	49	45	94

Source: GAO analysis of IRS data | GAO-16-590T

In commenting on drafts of the reports presenting the results of our fiscal year 2015 audit, the IRS Commissioner stated that while the agency agreed with our new recommendations, it will review them to ensure that its actions include sustainable fixes that implement appropriate security controls balanced against IT and human capital resource limitations.

We have also previously reported that IRS can take steps to improve its response to data breaches involving the inappropriate disclosure—or potential disclosure—of personally identifiable information. Specifically, in December 2013 we reported on the extent to which data breach policies at eight agencies, including IRS, adhered to requirements and guidance set forth by OMB and NIST.¹³ While the agencies in our review generally had policies and procedures in place that reflected the major elements of an effective data breach response program, implementation of these policies and procedures was not consistent.

With respect to IRS, we determined that its policies and procedures generally reflected key practices, although the agency did not require considering the number of affected individuals as a factor when determining if affected individuals should be notified of a suspected breach. In addition, IRS did not document lessons learned from periodic analyses of its breach response efforts. We recommended that IRS correct these weaknesses, but the agency has yet to fully address them.

IRS Faces Challenges in Addressing Identity Theft Refund Fraud

The importance of protecting taxpayer information is further highlighted by the billions of dollars that have been lost to IDT refund fraud, which continues to be an evolving threat. IDT refund fraud occurs when a refund-seeking fraudster obtains an individual's Social Security number, date of birth, or other PII and uses it to file a fraudulent tax return seeking a refund. This crime burdens legitimate taxpayers because authenticating their identities is likely to delay the processing of their tax returns and refunds. Moreover, the victim's PII can potentially be used to commit other crimes. Given current and emerging risks, in 2015 we expanded our high-risk area on the enforcement of tax laws to include IRS's efforts to address IDT refund fraud.¹⁴

IRS develops estimates of the extent of IDT refund fraud to help direct its efforts to identify and prevent the crime. While its estimates have inherent uncertainty, IRS estimated that it prevented or recovered \$22.5 billion in fraudulent IDT refunds in filing season 2014. However, it also estimated that it paid \$3.1 billion in fraudulent IDT refunds.

¹³GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

¹⁴GAO-15-290.

IRS has taken steps to address IDT refund fraud; however, it remains a persistent and evolving threat. For example in its fiscal year 2014-2017 strategic plan, IRS increased resources dedicated to combating IDT and other types of refund fraud. In 2015, IRS reported allocating more than 4,000 full-time equivalent staff and spending \$470 million on refund fraud and IDT activities. In addition, IRS received an additional \$290 million for fiscal year 2016 to improve customer service, IDT identification and prevention, and cybersecurity efforts.

The agency has also taken actions to improve customer service related to IDT fraud by, for example, providing an increased level of service to taxpayers calling its identity theft toll-free phone line. In addition, IRS has worked with tax preparation professionals, states, and financial institutions to better detect and prevent IDT fraud.

These efforts notwithstanding, fraudsters continue to adapt their schemes to identify weaknesses in IDT defense, such as by gaining access to taxpayers' tax return transcripts through IRS's online Get Transcript service. According to IRS officials, this allows fraudsters to create historically consistent returns that are hard to distinguish from one filed by a legitimate taxpayer.

These continuing challenges highlight the need for additional actions by IRS. As we have reported, there are steps IRS can take to, among other things, better authenticate the identity of taxpayers before issuing refunds. In January 2015 we reported that IRS's authentication tools have limitations.¹⁵ For example, individuals could obtain an e-file PIN by providing their name, Social Security number, date of birth, address, and filing status for IRS's e-file PIN application. Identity thieves can easily find this information, allowing them to bypass some, if not all, of IRS's automatic checks. After filing an IDT return using an e-file PIN, the fraudster could file a fraudulent return through IRS's normal return processing. Accordingly, we recommended that IRS assess the costs, benefits, and risks of its authentication options.

In November 2015, IRS officials told us that the agency had developed guidance for its Identity Assurance Office to assess costs, benefits, and risk of authentication tools. In February 2016, officials told us that this office plans to complete a strategic plan for taxpayer authentication across the agency in September 2016. Until it completes these steps, IRS

¹⁵GAO, *Identity Theft and Tax Fraud: Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks an Estimate of Costs, Benefits, and Risks*, GAO-15-119 (Washington, D.C.: Jan. 20, 2015).

will lack key information to make decisions about whether and how much to invest in authentication options.

Agencies with Government-Wide Responsibilities Play a Key Role in Guiding and Overseeing Federal Information Security

Under FISMA, the Director of OMB is responsible for developing and overseeing the implementation of policies, principles, standards, and guidelines on information security in federal agencies, except with regard to national security and certain other systems. The director is also responsible for coordinating the development of standards and guidelines by NIST.

For its part, NIST is responsible under FISMA for developing security standards and guidelines for agencies that include standards for categorizing information and information systems according to ranges of impact levels, minimum security requirements for information and information systems in risk categories, guidelines for detection and handling of information security incidents, and guidelines for identifying an information system as a national security system.

Accordingly, OMB and NIST have prescribed policies, standards, and guidelines that are intended to assist federal agencies with identifying and providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, alteration, and destruction of information and information systems, including those systems operated by a contractor or others on behalf of the agency. These include the following:

- OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*, which provides agencies with direction for managing information security risk on a continuous basis, including requirements for establishing information security continuous monitoring programs.
- NIST, Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.
- NIST Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information*

Systems, specifies minimum security requirements for federal agency information and information systems and a risk-based process for selecting the security controls necessary to satisfy these requirements.

- NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls.

OMB and NIST also have provided guidance to agencies on procedures for authenticating users to federal systems and websites, including the following:

- OMB M-15-13, *Policy to Require Secure Connections across Federal Websites and Web Services*, which requires all publicly accessible federal websites and web services to provide service through a secure connection.
- OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, which addresses federal government services accomplished using the Internet, instead of on paper, and calls for identity verification or authentication to make sure that online government services are secure and protect privacy. This guidance established four levels of identity assurance for electronic transactions requiring authentication. Each level describes the agency's degree of certainty that a user has presented an identifier that refers to his or her identity:
 - Level 1: little or no confidence in the asserted identity's validity.
 - Level 2: some confidence in the asserted identity's validity.
 - Level 3: high confidence in the asserted identity's validity.
 - Level 4: very high confidence in the asserted identity's validity.
- NIST Special Publication 800-63-2, *Electronic Authentication Guideline*, provides technical guidelines for federal agencies implementing electronic authentication and covers remote authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. Specifically, it provides technical requirements for agencies to use in selecting technology to achieve specified levels of e-authentication assurance, as defined by OMB and illustrated by the following examples:

-
- Level 1: Identity proofing¹⁸ is not required. Successful authentication occurs when an individual proves through the means of authentication that he or she possesses and controls the token.¹⁹ The cryptographic methods used at this level may still allow someone with malicious intent to intercept the transmission of a password through eavesdropping and crack it using a dictionary attack (i.e., guessing a password through trial-and-error using a dictionary).
 - Level 2: Requires single-factor remote authentication, using one of three factors—something you know (e.g., a password), something you have (e.g., an identification badge), or something you are (e.g., a fingerprint). Identity proofing requirements are introduced, requiring presentation of identifying materials or information. Approved cryptographic methods would not allow the type of eavesdropping attack that is possible at Level 1.
 - Level 3: Requires multi-factor remote authentication, requiring at least two authentication factors. An individual proves possession of a physical or software token in combination with some memorized knowledge. Approved cryptographic methods should be strong enough to protect against impersonation of the verifying entity.
 - Level 4: Is intended to provide the highest practical remote network authentication assurance, requiring the proof of possession of a key through a cryptographic protocol. At this level in-person identity proofing is required. It is otherwise similar to Level 3, except with stronger cryptographic methods in place.
-

OMB and DHS Are Responsible for Oversight of Operational Aspects of Federal Cybersecurity

Federal law also gives OMB and DHS responsibility and authority for oversight of operational aspects of federal information security. In

¹⁸Identity proofing is the process of verifying information about an individual for the purposes of issuing credentials to that individual.

¹⁹According to NIST, a token is something that an individual possesses and controls (typically a cryptographic module or password) that is used to authenticate the individual's identity.

particular, the OMB Director is charged with overseeing and enforcing agency compliance with information security requirements by taking certain actions authorized by relevant federal law (discussed in more detail below), and OMB has developed various mechanisms to carry out its oversight function.

- **Budgetary authority:** Federal law gives OMB the power of enforcement and accountability related to evaluating agencies' management of their information resources, which includes ensuring that information security policies, procedures, and practices are adequate.²⁰ In particular, in enforcing accountability, OMB is empowered to recommend reductions or increases in an agency's budget and restrict the availability of funds for information resources, among other things.
- **OMB Cyber Unit:** In fiscal year 2015, OMB established the OMB Cyber and National Security Unit (OMB Cyber) within the Office of the Federal Chief Information Officer. This unit is responsible for strengthening federal cybersecurity through oversight of agency and government-wide programs, issuing and implementing policies to address emerging IT security risks, and oversight of government-wide response to major incidents and vulnerabilities.
- **CyberStat Reviews:** OMB has also established the "CyberStat Review" process, which involves evidence-based meetings led by OMB to ensure agencies are accountable for their cybersecurity posture, while assisting them in developing targeted, tactical actions to deliver results.
- **FISMA reporting:** As required by FISMA, OMB reports annually to Congress on the effectiveness of information security policies and practices at executive branch agencies during the preceding year and a summary of evaluations conducted by agency inspectors general.

Regarding DHS, the Federal Information Security Modernization Act of 2014 codified its responsibility for certain operational aspects of federal agency cybersecurity. In particular, DHS is responsible for

- administering, in consultation with OMB, the implementation of agency information security policies and practices for information

²⁰40 U.S.C. § 11303(b)(5).

systems (other than national security systems, Department of Defense, and the intelligence community's "debilitating impact" systems);

- developing, issuing, and overseeing the implementation of binding operational directives to agencies on matters such as incident reporting, contents of agency's annual reports, and other operational requirements; and
- operating the federal information security incident center (the U.S. Computer Emergency Readiness Team or US-CERT), deploying technology to continuously diagnose and mitigate threats, compiling and analyzing data, and developing and conducting targeted operational evaluations, including threat and vulnerability assessments of systems.

In May 2015 DHS issued its first directive, which required all departments and agencies to review and mitigate all critical vulnerabilities on their Internet-facing systems. DHS identifies these vulnerabilities using scanning tools and reports the results to agencies on a weekly basis. Agencies are then required to mitigate the DHS-identified vulnerabilities within 30 days of the report, or provide a justification to DHS outlining barriers, planned steps for resolution, and a time frame for mitigation.

DHS has also supplied agencies with tools and technologies to assist in protecting against cyber threats and vulnerabilities. For example:

- **Continuous Diagnostics and Mitigation Program:** Since fiscal year 2013, DHS has provided agencies the opportunity to use a suite of tools and capabilities to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.
- **National Cybersecurity Protection System:** NCPS is an integrated system-of-systems intended to deliver a range of capabilities for intrusion detection, intrusion prevention, analytics, and information sharing. When deployed on an agency's connection to the Internet, the system monitors inbound and outbound traffic for malicious activity.

In summary, while IRS has made progress in implementing information security controls, it needs to continue to address weaknesses in access controls and configuration management and consistently implement all elements of its information security program. The risks IRS is exposed to

have been illustrated by recent incidents involving public-facing applications, highlighting the importance of securing systems that contain sensitive taxpayer and financial data. In addition, fully implementing key elements of a breach response program will help ensure that when breaches of sensitive data do occur, their impact on affected individuals will be minimized. IRS also needs to assess the costs, benefits, and risks of alternatives for better authenticating taxpayers who access its systems. Finally, strengthening the security posture of IRS—and other agencies—also depends on the key roles played by OMB, NIST, and DHS in providing oversight and guidance from a government-wide perspective, such as that related to improving authentication.

Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittee, this concludes my statement. I would be happy to answer any questions you have.

Contacts and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, Nancy Kingsbury at (202) 512-2928 or kingsburyn@gao.gov, or James R. McTigue, Jr. at (202) 512-9110 or mctiguej@gao.gov. Other key contributors to this statement include Jeffrey L. Knott, Larry Crosland, John de Ferrari, and Neil A. Pinney (assistant directors); Dawn E. Bidne; Mark Canter; James Cook, Shannon J. Finnegan; Lee McCracken; Justin Palk; J. Daniel Paulk; Monica Perez-Nelson; David Plocher; Erin Saunders Rath; and Daniel Swartz.

Biography

Gregory Wilshusen is Director of Information Security Issues at GAO, where he leads cybersecurity and privacy-related studies and audits of the federal government and critical infrastructure. He has over 30 years of auditing, financial management, and information systems experience. Prior to joining GAO in 1997, Mr. Wilshusen held a variety of public and private sector positions. He was a senior systems analyst at the Department of Education. He also served as the Controller for the North Carolina Department of Environment, Health, and Natural Resources, and held senior auditing positions at Irving Burton Associates, Inc. and the U.S. Army Audit Agency. He's a certified public accountant, certified internal auditor, and certified information systems auditor. He holds a B.S. degree in business administration (accounting) from the University of Missouri and an M.S. in information management from George Washington University's School of Engineering and Applied Sciences.

Chairwoman COMSTOCK. Thank you, and I thank all of you, and I now recognize myself for five minute questions rounds. We'll be having our questions now.

Mr. Koskinen, I'd like to read you a quote from Mr. George which said "It continues to identify"—TIGTA does—"significant security weaknesses that could affect the confidentiality, integrity, and availability of financial and sensitive taxpayer information."

Now, we have no choice—I've got my LifeLock but I've got to send it in anyway—to send in all our personal information to the IRS even though we don't know that you're not doing enough to secure that data, as we've heard here today. Can you right now assure the American taxpayers, our hardworking taxpayers who are going to be working over the weekend—because it's not due until Monday this year, so they're going to be turning it in on Monday—that the IRS information, you know, that their data is 100 percent secure?

Mr. KOSKINEN. I don't think there's any financial institution of any size in the world that can give you 100 percent guarantee. As you noted, the organized criminals we're dealing with are increasingly sophisticated and well-funded but I can tell you it is the highest priority for us. I can tell you that, knocking on wood thus far, our basic database, notwithstanding the over million attacks a day, continues to remain secure. We have not had a data breach into the database but we do not think that that necessarily means we can stop. In fact, we're using \$95 million of the additional funding that Congress gave us on cybersecurity to deal with in fact the issues that you've heard about, that is, continuous monitoring, being able to in fact segment our systems to protect them.

So all I can tell you is, we're doing everything we can at this point. The basic database has been secure. We hope it will be secure. But as I say, I can't give you 100 percent guarantee it'll always be secure.

Chairwoman COMSTOCK. Now, my understanding, and actually the Speaker was interested in this hearing as he's been interested in what's going on with the IRS, and he had asked about the IRS cybersecurity staff has been cut as the budget increased. Why did the agency cut its cybersecurity staff when they received additional resources?

Mr. KOSKINEN. That's an incorrect statement. The cybersecurity staff—all of our staff, we're down 15,000 people. We'll be down 17,000 people over the last five years because of budget cuts. The cybersecurity staff, the IT staff, in fact, has gone up somewhat. Our budget for IT has gone down \$200 million over the last five years. We are using the \$95 million of the \$290 million, as I said, for cybersecurity and we're hiring 55 additional new people in information technology to deal with cybersecurity. So there has been no significant cut in cybersecurity compared to anything else. We have far more people lost in revenue agents, officers and criminal investigators. So I would stress, when we've been given the money, and I think year will establish it, we put it to work effectively and efficiently. There are taxpayer dollars that deserve to be spent wisely.

Chairwoman COMSTOCK. Okay, and now who is the person who is in charge of cybersecurity at the IRS?

Mr. KOSKINEN. The person in charge of cybersecurity left a few weeks ago. He was one of the people on streamline critical pay, and without the reauthorization, we're trying to fill that spot. All of it reports to our Chief Technology Officer, also who will be leaving because of the expiration of streamline critical pay. It is important for everyone to understand, we have——

Chairwoman COMSTOCK. So right now the person who's in charge of cybersecurity is leaving and the person——

Mr. KOSKINEN. Has left.

Chairwoman COMSTOCK. Has left, and——

Mr. KOSKINEN. The person he reports to——

Chairwoman COMSTOCK. —the person who he's reporting to, the CTO, so the cybersecurity leadership has left the building?

Mr. KOSKINEN. We have people replacing them internally but what we need, as Congressman Lipinski said, Congress needs to give us the reauthorization to allow us to hire the highest skilled, capable IT security experts we can. We struggle otherwise. We find good people in the private sector and say if you'll sit there for three to six months while we work you through the process and fill out the applications, we'll be able to hire you, and these people are in great demand. Our people are in great demand. The people who are leaving are being recruited by the best companies in the world.

Chairwoman COMSTOCK. Well, certainly you've been aware of the problems here in cybersecurity given all the recent breaches, so when this—you know, you don't have these people now but what kind of planning had been going into this so you'd have that kind of talent pool when this expired, when you lost the people.

Mr. KOSKINEN. We have succession plans. We have replaced the Director of Cybersecurity on an acting basis but that's one of the reasons that the most critical request we have for Congress is to give us the additional support we need to bring people of the highest skills into the agency.

Chairwoman COMSTOCK. Okay. Now, have you talked with other agencies about how they're dealing with cybersecurity and——

Mr. KOSKINEN. We talk with them all the time. We work closely with the Department of Homeland Security, the Justice Department, the FBI, others, and——

Chairwoman COMSTOCK. And how often do you personally have meetings with these cybersecurity leaders within the agency?

Mr. KOSKINEN. I've met with the Secretary of the Department of Homeland Security and I've met with——

Chairwoman COMSTOCK. No, I mean with these people who just left. What type of meetings did you have sort of to emphasize that this was—you say it's a top priority so it's the top priority and we have the two people are leaving, I was wondering how often you were—okay, you guys are leaving, who do we have to replace and what are we doing for the succession plan?

Mr. KOSKINEN. I met with the Chief Technology Officer probably every two weeks. I have a regular monthly meeting with him for over an hour to review all of the matters of information technology. He participated in all of our senior executive meetings.

Chairwoman COMSTOCK. I see my time has expired. Now I'll recognize Mr. Lipinski for five minutes.

Mr. LIPINSKI. Thank you.

I want to say I'm—no one's happy here having to do their taxes right now, and fortunately my wife's an actuary and she takes over those duties. She'll be working on finishing this weekend. But I'm not here to beat up the IRS. I don't want to beat up the IRS. It's not my purpose. It's not because of the TV cameras here. But I think we need to know what has gone wrong and why, and get a guarantee that that is not going to happen again.

Now, there's no 100 percent guarantee of security. We know that. We have to accept that. We strive for that, hopefully everyone should be striving for that in both the public and private sector, but there's no 100 percent guarantee.

But I want to understand the reasons for the issues that Mr. George and Mr. Wilshusen had—the issues that they brought up such as the IRS didn't use the multifactor authentication, that the risk assessment wasn't done for IP PIN, and on top of that, there were two requests from TIGTA before IP PIN was taken down, and that there are 94 recommendations from GAO that have yet to be implemented. Why have these things happened? Is it a lack of understanding of the NIST standards, technical requirements? Is it a lack of ability within the IRS to do cybersecurity correctly? What is it that caused these issues in the past and why should we sit here and believe that those same things are not going to happen in the future, or is there something—is there anything wrong with what we've heard about these issues in the past? Is anything incorrect about those or did those happen, and why should we expect that they're not going to happen in the future?

Mr. KOSKINEN. As you noted, we're dealing with a moving target. Life is getting more complicated. The challenges are more sophisticated. When the Get Transcript application was designed and formulated in 2011 and 2012, the out-of-wallet questions were in fact a standard way of verification that was used by banks and financial institutions. The analysis was done, and the determination was made that at that time that was the appropriate authentication in light of the balance, as you know, between convenience for the consumers and the risks. As identify fraud and identity theft has increased and the sophistication has increased, it has become clear that questions that used to be answered only by the taxpayer now are actually more easily answered, although half the time the criminals can't even answer them. But I would note on the Get Transcript, 22 percent of legitimate taxpayers could not answer their own out-of-wallet questions, so it's not as if anybody could walk in and answer those questions. But it become clear over time that in fact more and more information was in the hands of the public and the out-of-wallet questions were no longer sufficient but that was not the decision and not the situation when it started.

I would note that we value and work cooperatively and collaboratively with the IG and GAO. Over the last few years we've had over 2,000 recommendations from them, and we work and we take them seriously, and in fact, we are implementing them as quickly as we can. As we move forward with the IP PIN, the determination was made, as noted, discussed with the IG, that it was an important service for people trying to file in January when they got their new PIN in January if they lost it to be able to access it. What we did was add another layer of authentication in the sense that we

marked every Social Security number when anybody got an IP PIN access, put that into a file, and every return filed with those Social Security numbers is put through a review. If there's any questions, we write taxpayers. A number of the letters the taxpayers are getting are to re-authenticate them before we will process those returns. As a result, we've determined that over 40,000—about 135,000 accesses were made. Forty thousand returns that have been filed have been authenticated as legitimate taxpayers. Over 5,000 have been stopped because they were fraudulent, and we determined those were fraudulent. We're continuing to review those as they are filed but we were satisfied at the start, and we discussed this with the IG in December and January, that the additional monitoring of literally every return against those Social Security numbers would increase our authentication ability.

In February, as we saw more volumes of what looked like suspicious access, because we were monitoring volumes as well, we agreed with the IG that we should bring the app down, and if anybody wanted their PIN we would mail it to them rather than having it accessible during filing season immediately. We are now, as noted, developing a multifactor authentication, which is difficult to do because we don't have immediate access to telephone numbers and other issues, but the tradeoff is, as I said, 22 percent of people couldn't get through to answer their own out-of-wallet questions. We think with the new multifactor authentication, it will be difficult for as many as 50 percent of taxpayers to get in but it will be much more difficult for the criminals. And so we're always in that balance of how difficult and burdensome will it be for taxpayers compared to how impossible can we make it for the criminal.

But it's an ongoing battle. As we design this system, it won't be the perfect system forever. We'll need to continue to monitor and assess what's happening. We'll need to continue the partnership we're developing with the private sector and with banks and others to compare notes about how we're doing. We continue to follow the NIST and OMB guidelines to the extent that they're there and, as I say, when we started with the IP PIN and Get Transcript 3 or four years ago, developing it, the standard was in fact being able to identify someone with out-of-wallet questions, and we've changed that and we're moving, but it's going to be more difficult for taxpayers.

Mr. LIPINSKI. My time is up right now. Hopefully we'll have a chance for a second round and we'll follow up on that and get the IG and GAO's response to any of that. Thank you.

Chairwoman COMSTOCK. And I now recognize the Chairman for five minutes.

Chairman SMITH. Thank you, Madam Chair.

Commissioner, recently the GAO made, I believe, 49 recommendations as to how the IRS could better protect taxpayers from being hacked, having their information hacked. This is on top of 49 recommendations that were made previously. My question is, how many of the 49 earlier recommendations have been implemented, and when do you expect all these recommendations to be implemented?

Mr. KOSKINEN. We're working on those GAO. As I said, we've had a couple thousand recommendations over time. GAO has done a very great service for us in the last year of prioritizing of the range of recommendations which are the highest priorities, and we are working on those. Our hope—

Chairman SMITH. How many of the 49 have you implemented so far, the earlier 49?

Mr. KOSKINEN. The earlier 49, I don't have that number for you. I'll have to get that for you. But our goal is to implement all of them. There's been some question about why we didn't immediately sign on to the most recent ones but the process is, we are supposed to advise Congress within 60 days of the detailed timeline, and we will provide you with the timeline for solutions to all of those.

Chairman SMITH. And the most recent 45 were just last month, and I realize you need some time to have them implemented, but I did hear you say you intend to implement them all.

Mr. KOSKINEN. Yes.

Chairman SMITH. In regard to the 49, how long will it take you to inform us as to how many have been implemented?

Mr. KOSKINEN. We'll be able to provide you that information in the next week.

Chairman SMITH. Okay. Why not in the next ten minutes?

Mr. KOSKINEN. Because I don't have that information with me. I'll have to get it from—

Chairman SMITH. Can some member of your staff sitting behind you get it for us before the hearing is over?

Mr. KOSKINEN. Some members of my staff sitting there can try to do that. We'd be delighted.

Chairman SMITH. Okay. Thank you for that.

Mr. KOSKINEN. Pardon?

Chairwoman COMSTOCK. I said we have computers and assistants here. They don't have paper with them.

Chairman SMITH. My next question, Commissioner, is this. I understand that the IRS issues refunds to individuals even when the names and the Social Security numbers don't match. Why does the IRS do that? It seems to me that you're catering to and perhaps even encouraging fraud. I understand there may be millions of individuals who are getting these funds to the tune of many, many millions of dollars. Why don't you stop doing that, or what can you do to correct it?

Mr. KOSKINEN. We actually don't issue refunds where there's a Social Security number on the return and a name that doesn't match.

Chairman SMITH. Okay.

Mr. KOSKINEN. I think the issue you're dealing with is people who aren't able to get a Social Security number file with an IP PIN.

Chairman SMITH. Correct.

Mr. KOSKINEN. And those IP PINs come in, and people who are paying taxes, a lot of them are in the country working without the ability to get a Social Security number. Their obligation is to pay taxes if there ever is a way for them to become citizens, the first question they're asked is, have you paid your taxes.

Chairman SMITH. But again, if the name and the Social Security number don't match, you are not issuing any refunds?

Mr. KOSKINEN. No, if the name and the Social Security number on the return don't match. Now, what the situation I think you're focused on is, people borrow, steal, however they get a Social Security number to get a job so their W-2 may have a different Social Security number but their name and the IP PIN, we grant the IP PINs. Those will match, and as long as they match, our responsibility is to collect the taxes people owe. It's not to in fact—

Chairman SMITH. But for example, I've heard—I don't know this is accurate—where someone would put in a Social Security number of 00000 all the way across and yet they are still getting refunds. Is that—

Mr. KOSKINEN. They can't do that on a tax return. The only thing they would be doing there is if they're using that Social Security number to get a job—

Chairman SMITH. Right. I understand. But still no refunds when there's a mismatch?

Mr. KOSKINEN. If you file a return with a Social Security and a name that don't match, we wouldn't give you a refund.

Chairman SMITH. Okay. That's good to know.

The next question is addressed to Mr. Wilshusen and Mr. George, and it is this. We've had a situation where something like over 700,000 people have had their tax information stolen, over 100,000 have had their Social Security numbers stolen, all in order to access an e-file PIN just this last year. What are the implications of that? What are the consequences of that? What does that say about the future and what can do about it? Mr. Wilshusen, we'll start with you.

Mr. WILSHUSEN. Well, one of the implications is that information could be used by criminals to commit identity theft and related financial crimes. It can also be used to help promote or facilitate identity theft refund fraud since they would have additional information that could potentially get past IRS's filters for trying to detect that type of fraud.

Chairman SMITH. Mr. George?

Mr. GEORGE. I associate myself with the comments that he just made, and this actually relates somewhat to a very important factor that hasn't really been discussed much today, and that is while we at TIGTA haven't found that the IRS's computers themselves have been breached as was indicated, the moment people are able to gain the name, Social Security number and other information, personal information, of taxpayers, that's really where the vulnerability exists currently to the system of tax administration.

Mr. KOSKINEN. And I might just add for the Chairman's benefit, the Social Security numbers that have been stolen and the identity information that's been stolen, all has been stolen someplace outside the IRS. Nobody is being able to get that information from us. The hacks have come from people masquerading already as taxpayers legitimately with Social Security numbers and names that match.

Chairman SMITH. Okay. Last quick question, if you'll address it yes or no. I'll address it to all three of our witnesses today. Is an individual's tax return and their personal information on that tax

return safer this year than last year? Commissioner, what would you say?

Mr. KOSKINEN. Yes, safer.

Chairman SMITH. Mr. George?

Mr. GEORGE. I have no indication that that is not the case.

Chairman SMITH. Okay. Mr. Wilshusen?

Mr. WILSHUSEN. I wouldn't be able to comment on that but I would probably say I have no evidence to show it's higher or lower.

Chairman SMITH. It may be the same. Okay. Thank you, Mr. Chair.

Chairwoman COMSTOCK. I now recognize Mr. Tonko for five minutes.

Mr. TONKO. Thank you, Madam Chair, and welcome to our guests, and I believe that the information exchanged here is very critical, and it's important to protect taxpayer information. I think that we all bear that sort of responsibility and goal, and I thank you for the information again.

Can I just get a better sense of the IT budget for perhaps the last five years or so from 2010? Has it been flat? Has there been a decrease, increase? What basically are we talking about in numbers here?

Mr. KOSKINEN. Even after the money that we appreciated Congress added this year, the \$290 million, we're still \$900 million below where we were six years ago, so we have 10 million more taxpayers, we have a set of unfunded mandates including the Affordable Care Act, FATCA, the ABLE Act, private debt collection that we're implementing with \$900 million less, and as I said, 15,000 fewer employees.

Mr. TONKO. So the efforts here to go forward I would think some of it is a function of having resources essential to address some of the dynamics perhaps a pay scale differential with the private sector to compete for the talent. Can we talk about that for a bit, your efforts with a skilled cybersecurity workforce? How do you address the whole impact of strengthening that given that the private sector may have that pay differential?

Mr. KOSKINEN. Well, the Restructuring Act of the IRS was implemented in 1998, the IRS was given special authority for 40 places, 40 positions called streamline critical pay, which allowed us to hire people as if we were in the private sector, bring them right in without going through the 3 to 6 months of hiring, and allowed us to have a differential pay, not enough to match the private sector, but we have found, because we have so many challenges in such a large organization, a lot of people with IT backgrounds and the people we've been able to hire want to come work for the IRS. So one of the great concerns we have about the loss of that authority is our ability to compete with the private sector, and not on dollars but really on the combination of appropriate pay and a very great challenge in IT has been diminished with the failure to reauthorize that streamline critical pay. It's only 40 positions. We never used all 40 of them. The most we ever used was 34.

The IG a year and a half ago reviewed the program and said it had been run appropriately, and so we view it as critical because we are the largest financial institution in the world. We collected last year \$3.3 trillion. We are the most attractive database to at-

tack because we've got information on 300 million Americans. So our sense is, whatever support we can get in this regard is very important.

Mr. TONKO. And in the last 5 or six years you've had to make up a decline in revenues, resources with the shot that you got, the one shot you got last year, but that must have impacted somehow addressing the differential.

Mr. KOSKINEN. Yes. So what happens is, as a result across the board we have to prioritize. Cybersecurity, identity theft, protection of taxpayer data is a high priority. As I said, we've actually had more people in IT while we've lost thousands of other employees. But it does mean, for instance, on patches, there are thousands of patches—we have a very complicated system—that come in every year and we have to prioritize which we can implement because we actually have a limited amount of resources. That's why we appreciate the work that both the IG and GAO do helping us prioritize of those security updates, which are the most critical that need to be improved immediately.

Mr. TONKO. And so other than the workforce issue, what are those reforms or those improvements? Where do we need to reach? What are the tools in the toolkit that are required to provide for taxpayer protection here?

Mr. KOSKINEN. But we're continuing to work, as I say, to implement the recommendations that we have and that we get from the IGs and GAO. As I say, we need to improve, and part of the money we're spending this year out of the 290 is to improve our continuous monitoring of the system. We're working on segmenting the system so if you actually happen to get into the database, you can't run barefoot through it all. We'll actually—you'll only be able to get into limited parts of it. We're working to improve the security, as noted by GAO. I don't have it with me, but you can run—I can't access my computer, not with—I don't need passwords, I have to actually put an identity card into the computer. Part of the money we hope to use if we get it for 2017 would be to have that same access code requirement for access to all of our internal systems. As GAO noted, we're as worried and focused on internal protection as we are on external protection.

Mr. TONKO. Thank you very much. I have used up my available time, but I appreciate the efforts that are being made. And again, bearing in mind that taxpayer protection should be the guiding force, I appreciate the response to the questions here.

And with that, I yield back, Madam Chair.

Chairwoman COMSTOCK. Thank you.

And I now recognize Mr. Lucas for five minutes.

Mr. LUCAS. Thank you, Madam Chair.

Mr. Wilshusen, let's talk for a moment about the magnitude of the fraud. According to your testimony, the IRS estimated that it prevented or recovered \$22.5 billion in fraudulent identity theft refunds in 2014 but paid out \$3.1 billion in fraudulent refunds. These numbers seem rather precise considering there's no range given. How does the IRS estimate how much it's prevented in fraudulent payments and how much has been paid? And how confident are you, I should say, on the accuracy of these numbers?

Mr. WILSHUSEN. Well, uncertainly exists with any estimates with regard to the amount that has been paid or that has not been detected and not paid. IRS provides a rather specific point estimate. However, because you really don't know what you don't know, there's likely to be undetected fraud that hasn't been determined. So there's always uncertainty with those estimates, and that's why we recommended that IRS look at its estimating procedures to account for that uncertainty as to the extent of the fraud.

Mr. LUCAS. Mr. George, fraudulent tax payouts ultimately hurt taxpayers because their public money is going to criminals. How confident are you that the IRS has a grasp on these estimates? And does this raise concerns about whether the IRS is allocating enough resources to combat the identity theft problem?

Mr. GEORGE. This is a very complicated question, Congressman, because it overlaps with a lot of other issues as it relates to monies owed to the Internal Revenue Service. The Service itself estimates what it calls the tax gap at being over \$450 billion every year, money that is owed to the IRS that no one has really contested that figure. And so it's a serious problem.

Then, of course, you're talking about programs such as refundable credits and the like that are being taken advantage of by people who are here in this country both legally and illegally.

So it is a major problem. The IRS is aware of it. I'm sure the Commissioner will point out that if he had additional resources, he would be able to address it more sufficiently. But this is a concern that we've raised extensively during my tenure at TIGTA.

Mr. LUCAS. Thank you, gentlemen.

Madam Chairman, actually, I yield back.

Chairwoman COMSTOCK. And I now recognize Mr. Abraham for five minutes.

Mr. ABRAHAM. Thank you, Madam Chairman.

I think this hearing may be the best argument for a simpler flat-tax-type deal because we look at OPM, we look at the IRS, ACA, every government agency recently in the last year or 2 or 3 at the most seems to have had a major data breach. And every time it starts out with a lower number such in your case with the IRS, the 300, then it goes to 7. Same thing happened in the OPM. It started out a few million, went up to 24, 25 million.

So, again, you know, I personally—and I think everybody listening to this hearing—would rather be responsible for their own security because, you know, our agencies are having major problems getting it right. And again, when we—I'll talk to you, Mr. Koskinen, about you guys—you know what you need to do. I mean, from a single identification to a multiple, I mean, that's pretty commonsense stuff. And it's not like these things were born of yesterday. I mean, these things have been going on for a long time.

But I know you guys are asking for more money, so help me out here. Of the \$290 million that we as Congress gave you for this fiscal year 2016, I'm told—and you can certainly correct me if I'm misstating—but how much of that went to employ temporary people to help on the toll-free line?

Mr. KOSKINEN. I would note, by the way, that government agencies are challenged, everybody is challenged, Target, Anthem, J.P. Morgan Chase—

Mr. ABRAHAM. I understand that, but, I mean, we've been—you know, we've been here so many times.

Mr. KOSKINEN. Yes.

Mr. ABRAHAM. We just keep going to the same well and the water keeps coming up dry so——

Mr. KOSKINEN. So with regard to the \$290 million, which, again, I would say we appreciate it. It's a step in the right direction. One hundred and seventy-eight million was devoted to taxpayer service. Last year——

Mr. ABRAHAM. Right. So is that about 1,000 employees?

Mr. KOSKINEN. So we hired slightly over 1,000 employees, temporary employees. We hire eight to 10,000 temporary and seasonal employees——

Mr. ABRAHAM. Yes.

Mr. KOSKINEN. —to help with filing season.

Mr. ABRAHAM. And I guess my point is that \$178 million did not go to specifically fight cybercrime?

Mr. KOSKINEN. No. The other then of the \$178 million, \$95 million went to cybercrime——

Mr. ABRAHAM. Right.

Mr. KOSKINEN. —and another \$16 million went to identity theft, primarily to support our partnership with the private sector and the States.

Mr. ABRAHAM. All right. So I'm doing the math and certainly won't—don't want to disparage any employee at the IRS. I'm sure they hopefully earn their money every day. But 1,000—the \$170 million, that's \$178,000 per employee. Is that the normal salary? I mean, I may want to——

Mr. KOSKINEN. No.

Mr. ABRAHAM. —apply there.

Mr. KOSKINEN. I'd apply there. That's more than I make. No, the \$178,000 includes all of the supporting issues that go with it. The major expenditure was the 1,000, but they get paid in the 30, 40, \$50,000 range. The \$178 million that was spent there was all of the supporting systems to in fact get our level of taxpayer service up from last year's 37 percent to this year's 72, 75 percent. So you can actually get somebody on the line within a few minutes this year. Last year, you had to wait for 30 to 40 minutes. Sixty percent of people couldn't get through it all.

Mr. ABRAHAM. Okay. And I know that OMB required you guys to reassess and look back at your security procedures, and I guess the question, again going back to the earlier statement, why don't you guys conduct an authentication process with your IP issue, your IP PIN problem? Did you all review, did you look ahead? Why didn't you follow OMB guidelines?

Mr. KOSKINEN. We actually followed OMB guidelines and the NIST guidelines as well when we were establishing these programs. As I noted, what happens is life gets more complicated as you move along. What used to be acceptable no longer works.

With the IP PIN, as I noted, we brought it back up this year because we added another level of authentication. We monitored every return filed as a result of anybody accessing that system, and therefore, we're reasonably confident and as our life has shown, the

vast majority of people using those IP PINS are legitimate taxpayers.

We ultimately brought it down when our monitoring of each one of those accesses identified that there were an increasing number of criminals trying to get through and the vast majority of criminals couldn't get through, and so we shut it down, deciding that, while it was a great convenience to taxpayers, at that point it needed to be brought down because of our concerns about the security.

Mr. ABRAHAM. Thank you, sir.

Thank you, Madam Chairwoman. I yield back.

Chairwoman COMSTOCK. Thank you.

And I now recognize Mr. LaHood for five minutes.

Mr. LAHOOD. Thank you, Chairwoman. And I want to thank the witnesses for being here today, for your testimony.

Commissioner, you know, as an outsider looking in and looking at what we've heard, 700,000 taxpayers having their personal information compromised, that we had the GAO come in with 45 recommendations that, you know, the Chairman asked you how many of those have been implemented, and we didn't get a sufficient answer on that, and then more recommendations from GAO. And I guess, I mean, what are the successes that you've had in fixing this problem? I mean, when we tell the American people we've had successes, we're fixing this, we're giving you confidence that we're on the right track after we've had these series of events, statistics out there, and these breaches, I mean, what are the successes?

Mr. KOSKINEN. The successes are, first of all—and again, I always knock on wood—our basic system has not been breached. As I say, we are attacked over a million times a day.

Mr. LAHOOD. Since when? When is the date that you use on that?

Mr. KOSKINEN. Forever. We've not had a breach of our database directly. We've had breaches by people masquerading as taxpayers and applications. The basic database of the IRS has had no significant breach that I know of ever.

But the other thing that's happened, we're talking of identity—we are increasingly successful at stopping refund fraudulent returns. Last year, we stopped over four million suspicious returns, 1.5 million of them for about \$8 billion were identified as fraudulent. Our ability—our filters are going forward.

The most significant thing we've done in the last year, very successful, is our partnership with the private sector and the States, working together for the first time, exchanging information in real time during the filing season of where do they see suspicious patterns, where do we. We are sharing that back-and-forth. A small part of the money that we got for the \$290 million is being spent in support of that partnership.

I think the data will show that this year taxpayers were safer. I was asked that question. And the reason I'm confident about that is that for the first time we have a level of authentication for taxpayers when they go to their preparers or when they use software. We have increased data that we get now that we get now that we didn't used to be able to have access to of where the returns are coming from and how many are coming from individual computers all through our private sector partnership so that we have, as I

say, taken the entire tax system and put it together in a unified attempt for the first time ever, in a partnership, in in a true public-private partnership.

Mr. LAHOOD. So the 700,000 that have had their personal information compromised, I mean, when did that change in terms of the implementations that you've made and that we're not seeing the numbers that have been compromised? I mean, has that changed since when?

Mr. KOSKINEN. I'm not sure I quite understand. The 700,000 successful accesses by criminals in our "Get Transcript" took place over a period from 2014 to '15. We originally looked at the immediate impact with the IG then with them. They collected data for us for the entire time. That system is down. When it comes back up, it will be much more secure and also much more difficult for taxpayers to use, but that's the tradeoff we continually have to make.

Mr. LAHOOD. And then one thing that I haven't heard you talk about is—so we've talked about these hackers and the criminals. I mean, tell me about the successful prosecutions that you've had in terms of the deterrent effect if we're going to stop this from going forward, the successes you've had with—successful prosecutions going after people that you can kind of hold out that we've stopped this and these people are being held accountable?

Mr. KOSKINEN. We've put over 2,000 people in jail in cooperation with the IG and the Department of Justice. Our criminal—

Mr. LAHOOD. And can you give me a couple examples of kind of highlighted cases and the effect that that's had?

Mr. KOSKINEN. I get reports of those every day. Those are people who have created syndicates. They filed \$100 million worth of false returns. They've filed large numbers. The courts have been very supportive. The average time of incarceration is over 3-1/2 years for each of those convictions. They are widely publicized. As I say, I get a list of them every day. I would be delighted to give you—we just put out—about three or four weeks ago the Criminal Investigation Division put out a release which I'd be happy to get you of the 10 most significant criminal prosecutions for identity theft and refund fraud.

Mr. LAHOOD. And have you found that the criminal code right now in terms of the senses people are getting, is it having a deterrent effect? Does that need to change? Are there recommendations on that?

Mr. KOSKINEN. At this point we think that the courts and the code have been sufficient on that ground. As I say, part of what's happened as we've, I think, begun to be successful at stopping criminals locally, increasingly what we're discovering is we're dealing with organized crime syndicates in Eastern Europe and Asia where it's much harder to get prosecution. The people that are operating with them here are basically relatively low level. We have over 1,700 investigations going on right now leading toward further criminal prosecutions, but at this point I don't think increasing the severity of the penalty for fraud is a need for us. As I say, the courts have been very good. Average sentence—some sentences have been in the range of 10 to 20 years.

Mr. LAHOOD. Thank you. Those are all my questions.

Chairwoman COMSTOCK. Okay. I now recognize Mr. Hultgren for—oh, he's not here now. Okay.

Mr. Moolenaar for five minutes.

Mr. MOOLENAAR. Thank you, Madam Chair, and I appreciate the panelists today.

And, Mr. Wilshusen, I wanted to just—your role at GAO has to do with accountability, especially in the—sort of the information technology area, is that correct?

Mr. WILSHUSEN. That's correct, on information security, cybersecurity issues.

Mr. MOOLENAAR. So because you're probably looking at this over a wide range of agencies and government entities. I basically have three questions that I'd like to kind of lay out for you and you'll kind of get the pattern of where I'm going with these questions. So you might want to just take notes just so you—I apologize for overwhelming you with three questions at the same time.

But basically I just wanted you to elaborate on the testimony you've already given just so I have a clear understanding. But the first question is what potential enforcement and accountability options could be applied against an agency that is noncompliant with OMB and NIST information security standards and guidelines? That's kind of the one question, you know, what options are available?

And then secondly, what federal agency or White House office might have the authority to enforce compliance with OMB and NIST standards and guidelines? So who has the authority to implement that?

And then finally, and thirdly, are you aware of any cases when action was taken against any agency for failing to comply with OMB and NIST information security standards and guidelines?

Mr. WILSHUSEN. Okay. First, I would answer those questions in order. In terms of enforcing compliance or holding agencies or individuals accountable for implementing information security, it starts first at the agency with the head of the agency. FISMA, the Federal Information Security Modernization Act of 2014, requires the head of the agency and assigns overall responsibility to the head of each agency to ensure that that agency implements appropriate safeguards to protect against the unauthorized use, disclosure, modification of information within that agency. The head of the agency is also responsible for enforcing and ensuring that individuals and employees within that organization are held accountable and comply with that policy and with those procedures.

Some of that responsibility has been delegated to the Chief Information Officer. In some respects at agencies, the Chief Information Security Officer will have some responsibilities to help program managers and assist them in complying with the procedures.

At the government level, it's the Director of Office of Management and Budget, who under FISMA, has responsibility for assuring and enforcing the compliance of information security under the law. The Office of Management and Budget they have employed several different mechanisms to help provide accountability and, if you will, assistance to federal agencies. One of these is through the budget process in which OMB can recommend changes to proposed

budgeted amounts for organizations and agencies to help assure that information security policies are being implemented.

It's also through cyber stat meetings, which the Office has established, in which OMB will meet with officials from individual agencies to talk about weaknesses or issues of concern related to information security at that agency with those officials from that agency. And it's intended not only to hold those officials accountable to some extent but also to assist them in implementing the appropriate security controls.

OMB also provides a reporting mechanism through the FISMA annual reporting mechanism in which OMB reports on agencies' progress in implementing information security controls, as determined by the metrics that OMB has determined.

So those are at least some of the options that are available, in terms of what federal agency has that enforcement—well, first of all, it's within—you know, each agency has responsibility, as does OMB, and so they have a responsibility to perform those functions.

In terms of actual actions taken, well, OMB does have the cyber stat reviews. It holds them annually with several organizations. But in terms of holding someone accountable in terms of like firing someone if that's what you're referring to or actually reducing the budget of an organization, I don't know if OMB has done that. I know over the last several years the actual budgets for information security have been increasing rather than decreasing.

Chairwoman COMSTOCK. Thank you. And I now recognize Mr. Westerman for five minutes.

Mr. WESTERMAN. Thank you, Madam Chair. Good morning, Commissioner and panel.

You know, I attended the prayer breakfast this morning and seeing the Commissioner here in this special time of season reminded me of life's two certainties of death and taxes. But, you know, I think there may be—

Mr. KOSKINEN. I'd like to note we're the tax part of that.

Mr. WESTERMAN. I'll leave that one alone, but there may be a third part, there may be a new certainty in life and that is that your personal identifiable information is going to be stolen at some point.

When the current e-authentication framework was being developed, the National Institute of Standards and Technology informed the IRS that a taxpayer identification number was an acceptable form of identification. Now, I'm going to get real acronym-heavy here because as slow as I talk, there won't be time to answer if I didn't use these acronyms.

In August 2015 NIST informed TIGTA that a TIN is now not an acceptable government identification number for the purpose of authentication. IRS agreed with this update and indicated the agency would take steps to conform to NIST standards.

So my first question is when and how did NIST initially inform the IRS that a TIN was acceptable?

Mr. KOSKINEN. It was accessible?

Mr. WESTERMAN. Was acceptable.

Mr. KOSKINEN. It was acceptable, again, when the programs were developed in 2011 and '12. It was part of a general framework. I'm not aware of a particular NIST approval. NIST sets out

standards that we're obligated to and do follow. It doesn't necessarily, that I'm aware of, do reviews and respond to particular questions. But we did, through the IG, understand that NIST's view by last summer was that, by that time, because as you noted, so much personal information has been stolen and in the hands of criminals, by itself, a taxpayer identification number was no longer acceptable. And by that time we had taken the "Get Transcript" down.

Mr. WESTERMAN. All right. So that was in 2011, you said, when it was—

Mr. KOSKINEN. 2011 and '12 when we designed the system. Taxpayer identification numbers and out-of-wallet questions were being used by a range of financial institutions and others for authentication.

Mr. WESTERMAN. So what steps have you or the IRS taken with this communication you've had with TIGTA to conform to the NIST standards? Are you saying you're not aware that they're—

Mr. KOSKINEN. No, in light of that and our experience have taken down the "Get Transcript" application, the IP PIN application. We are in the process right now of testing a multifactor authentication process that will require taxpayers to identify themselves through an additional factor. We'll communicate with them with their cell phones or smartphones or other devices that we've not had access to before, and they'll have to come back through with a PIN and identifier, reinforcing all the other information they'll still have to provide us. That system we hope to have up in the next two or three months, perhaps earlier, and that will in fact be at the highest level and the appropriate high level that NIST now has out there. It's called multifactor authentication.

Mr. WESTERMAN. Okay. And, Mr. George, is the current e-authentication framework compliant with NIST standards? And if not, does that mean that other online services such as online payment agreement, Direct Pay, and Where's My Refund are more vulnerable to compromise?

Mr. GEORGE. They're vulnerable to compromise, but the impact on the taxpayer is not the same. If someone wants to find out where their refund is, it won't affect—even if it's an impersonation type of a situation, that won't affect the amount of money involved here. I mean, they might get additional information that ultimately could be misused if one of the factors to authenticate who the taxpayer is is what was your refund last year.

Mr. KOSKINEN. But you can't access the app without knowing what the refund was.

Mr. GEORGE. Right.

Mr. KOSKINEN. It's a good point because authentication depends on the nature of the risk. When our assumption is if you're going to pay us on an online payment agreement, you're unlikely to be a criminal. Criminals don't usually send us checks. If you're checking for a piece of information like where's my refund, you have to actually know what the refund is that you're asking about. You can't just go in and say have I got a refund coming. You have to put all of your personal information in and you have to identify the exact dollar amount of the refund to find out where it is. We had

about 250 million hits on that app already this year. Those people used to have to call.

Mr. GEORGE. Now, keep in mind also—and this should've been stated at the outset—there's the figure of 700 or 400,000, 800,000. That number is not accurate because if someone gets access to information under the "Get Transcript" application when it was up and running, they also have access to dependent information and spouse information, so that number could be exponentially higher in terms of potential victims of identity theft or any other taxpayer mischief.

And then ultimately, again—and I'm glad that the Commissioner—and he and his staff have been extraordinarily cooperative, Congressman. But the IRS simply misjudged the risk of the processes that they had in place when they first instituted the "Get Transcript" program. They thought it was a very low-risk endeavor, and it obviously turned out not to be the case.

Mr. WESTERMAN. I yield back, Madam Chair.

Chairwoman COMSTOCK. Thank you.

And I now recognize Mr. Palmer for five minutes.

Mr. PALMER. Thank you, Madam Chairman.

Mr. Koskinen, one of the potential vulnerabilities that concerns me is that government employees have access to the federal system to access their personal emails, you know, Facebook, Web sites, you know, online shopping using the federal network. Has the IRS taken any action to restrict access by their employees?

Mr. KOSKINEN. I'm not sure—

Mr. PALMER. In other words, do you allow your employees to use the federal network for personal use?

Mr. KOSKINEN. No. Actually, you can't do personal email at home and your government email is to be used for government purposes. We are very strict about no one does work on their own personal computer. They may do other things with their personal computer. But basically, we restrict Web sites. We are actually now taking another look at should we restrict even access to more Web sites than there are now. But as a general matter, people do their personal work on their personal computers, do office work on their office computers.

Mr. PALMER. Thank you. Do you have a written policy that you could provide the Committee?

Mr. KOSKINEN. A—I'm sorry, a—

Mr. PALMER. A written policy to that effect?

Mr. KOSKINEN. Written policy about that, I'd be delighted to provide it to you.

Mr. PALMER. Thank you, sir. Last week, I had opportunity to tour the Center for Information Assurance and the Joint Forensics Research at the University of Alabama Birmingham. The Center is doing fantastic work under in the cybersecurity field and producing talented students with the ability to make a real difference in the field. It's under the leadership of Gary Warner.

The thing that disturbs me in this is that, despite the government's tremendous need for individuals with this skill set, the Director of the Center explained that he has students applying for jobs at the federal agencies who don't hear back from them for months and they wind up getting jobs in the private sector. And

I'm talking about some of the very best. I want to know if the IRS has taken any steps to expedite the interview process for people with a skill set that we definitely need?

Mr. KOSKINEN. All right. Well, certainly in that area, as a general matter, as I say, our problem is we are not hiring very many people at all. We'll shrink by another two to 3,000. The only way we've been able to deal with the budget cuts, since 70 percent of our budget is people, is simply not replace people. That's how we've shrunk by that much.

But IT is an area where we're trying to hire. The process you mentioned is in fact, when you apply for a job in the government, you go into the normal process, it takes three to six months. Many times, it's several weeks or months before you hear back when you've applied, and it's why, as we discussed earlier, for us at the senior level of trying to get the best people, the streamlined critical pay authority is so critical because nobody is in greater demand than cybersecurity experts, and if we tell them it's going to take you 3 to 6 months but just sit tight and we really want to hire you, by the time we get back to them, you know, they're not there anymore. And I think that I take your point.

Mr. PALMER. Yes.

Mr. KOSKINEN. We have fewer than 300 people under age 25 in the agency because we've not been able to hire. So those are exactly the kind of people that we would love to hire and we ought to be hiring and that we ought to be able to try to figure out how to get into the system.

Mr. PALMER. Madam Chairman, I don't know what our responsibility would be through the Committee, but I would like to recommend that we develop a procedure that would expedite the interview process for such critical personnel so that we could get more of those highly skilled people into places where they can help protect our IT systems.

Mr. Wilshusen, according to your testimony, the IRS estimated, prevented, or recovered \$22.5 billion in fraudulent ID refunds, identity theft refunds in 2014, but paid \$3.1 billion in fraudulent refunds. I don't know if the GAO has looked into this, but those numbers are fairly obvious. It's money that's leaving the system. But do you have any idea what it costs the IRS to engage in prevention and recovery activities? Because that's an additional cost to the federal government.

Mr. WILSHUSEN. I do not.

Mr. PALMER. Chairman Koskinen, do you?

Mr. KOSKINEN. On cybersecurity, generally, we spend about \$150 million a year just on cybersecurity. We have about 3,500 people working on identity theft, devoted to that. We've never pulled together the full cost of protecting against identity theft and refund fraud, but it's obviously money well spent if we're able to stop \$25 billion from going out the door.

Earlier, there was a question on how accurate are those numbers. We're pretty good at knowing which refunds we stopped. The point is a good one. We can tell which refunds got out when somebody—a legitimate taxpayer comes in. There's always an uncertainty of which fraudulent refund went through where there was no competing filing.

Mr. PALMER. If—

Mr. KOSKINEN. Those are the ones you don't know.

Mr. PALMER. What I'd like for you to do if you don't mind is to provide the Committee with at least an estimate of what you're spending on recovering fraudulent refunds.

Mr. KOSKINEN. Sure.

Mr. PALMER. Madam Chairman, if I may, I have one more question.

Mr. Wilshusen, in the area of information security controls, how many recommendations has the GAO made to the IRS and how many of those recommendations remain unimplemented? And how far back do those recommendations go?

Mr. WILSHUSEN. Okay. We have recommendations that remain outstanding and open that go back to our report in 2011 and 2012 and so some of those recommendations actually pertain to filing seasons or fiscal years from like 2010, 2011. We have right now 94 open recommendations, but that includes 45 new recommendations that we just made in March. And so other than those, we do have 49 other recommendations that have been open for over a year.

Mr. PALMER. Mr. George, same question, recommendations from the IG's office?

Mr. GEORGE. Yes, I don't have off the top of my head the exact number, but there are quite a few, and we have, for the benefit of the IRS, prioritized those recommendations. Well, I was just pointed out that as of March of this year the IRS has 23 open recommendations from 14 audits that we've provided them between the years 2008 and 2016.

Mr. PALMER. My final question, and I promise this is the final one, is a follow-up to Chairman Koskinen. Why is the IRS unable to implement these GAO and IG recommendations? Assuming that the agency concurs with them, when do you expect the IRS to fully and successfully comply with the GAO and TIGTA recommendations?

Mr. KOSKINEN. As I say, we value the partnership. I've always been a fan of internal auditors in the 20 years in the private sector as well. Our analysis is—for another purpose was that we've had about slightly over 2,000 recommendations from the IG and GAO across a wide range of areas, and about 80 percent of those have already been implemented.

In the security area, again—and the IG has started moving that way—for both GAO and the IG, the ability to prioritize those for us as to which they think are the most critical allows us to then prioritize our work. We're limited obviously by just time as well as resources, but time is one of them. But we are committed in the security area to implement those as quickly as we can.

And we will be providing Congress a report as quickly about the most recent GAO recommendations. We, 60 days afterwards, provide GAO and the Congress our timeline as to exactly what the recommendations are and when they'll be implemented, and we'll be providing you that report.

Mr. PALMER. Well, my final comment will be this: that when you have recommendations from the IG's office that go back to 2008, that would indicate to me no intention to implement them.

I yield back. Thank you for your indulgence, Madam Chairman.

Chairwoman COMSTOCK. Thank you.

We're going to do a second round of questioning for those who might want to stick around. And so I now recognize myself for five minutes.

I did want to pick up on—Mr. Wilshusen, you had indicated the increased budgets. I just want to make an observation actually. In the report that the speaker had actually cited and asked the question about—that I had asked was from Hill newspaper articles saying the IRS cybersecurity staff was cut as the budget rose and that was also—they referenced an IG report that you had done, Mr. George, that it was also a cybersecurity online report that referenced that also. So I'd like to just put that into the record in recognition of what you all had said.

[The information follows appears in Appendix II]

Chairwoman COMSTOCK. But I also wanted to pick up on what you testified about, Mr. Wilshusen, about the agency using easily-guessed passwords, software patches not being done, and you had said the IRS had inconsistent execution. Would this—put it in a little more simpler way that people just weren't doing their jobs. The people who were there, regardless of what budgets and what things are being done, I mean, those are basic cyber hygiene things that we've all heard about. I mean, we're very familiar from the OPM breach and the hearings we had here.

So when I hear these kind of things that are very common and the inconsistent execution really being people not doing their jobs, would that be a correct assessment?

Mr. WILSHUSEN. Well, I think you're absolutely correct. These are very common types of security practices that need to be implemented. And they were not being consistently implemented across the IRS. We think there are probably several reasons why that occurs. In some respects, for example, we looked at the IRS's security testing and evaluation procedures, and we noted that they weren't always that successful in identifying the same type of vulnerabilities that we identified.

We also noted that when IRS implemented, for example—said that it had implemented 28 of the recommendations that we previously made, that it had not actually implemented nine of those. That's a reflection of its information security practices or its practices for closing our recommendations before they were actually implemented.

So there's probably a number of reasons why these conditions continue to exist, and certainly not performing those functions and responsibilities in an appropriate manner contribute to that.

Chairwoman COMSTOCK. And I'd like to ask you and Mr. George, given that right now there's basically no one in charge of cyber at the IRS from what we've learned today—

Mr. KOSKINEN. I think that's unfair. That's not what I said.

Chairwoman COMSTOCK. Well, I'm asking Mr. Wilshusen and Mr. George where we—is that—in terms of—you were asked earlier about the safety. When these basic things that you're seeing—and when they're telling you 28 of them have been implemented but nine of those haven't, their own self-assessment is inaccurate, you tell them what to do. The inconsistent execution—I mean, execu-

tion is doing your job and being able to do these basic tasks. Do you have confidence that you're going to see this anytime soon?

Mr. GEORGE. Madam Chairwoman, we did make a recommendation, which the IRS agreed to. The one kink in their armor was that there was not a service-wide approach to cybersecurity. A particular unit had a dedicated division that would interact lightly with other units within the Internal Revenue Service, but it wasn't across the board. And my understanding is that the IRS and the Commissioner has agreed to change that.

Mr. KOSKINEN. And we've implemented that.

Chairwoman COMSTOCK. And I would just note that, you know, we had OPM before us—the Commissioner also noted that in the private sector these things happen, but I would note that Ms. Archuleta is no longer working at OPM. As our other CEOs of companies where they had these major breaches, they were not working there. So while—you know, Ms. Archuleta did move on.

And I think when we look at these issues, I don't have confidence. I can't go back to those people, more than half of whom in my district raised their hands when we hear about these letters and their breaches, they certainly didn't have confidence in OPM, and I know they don't have confidence with the IRS. This is a pretty important area where we need to have confidence, and I don't see it there.

And I think you've had other people move on when they aren't having consistent execution of their jobs, and I think what we've seen here today is not a lot of consistent execution at all or confidence that there will be going forward.

So I will yield back my time. And if Mr. Lipinski—thank you.

Mr. LIPINSKI. Thank you. There's a couple things I wanted to go back to that have been mentioned. First, I want to ask—and the Commissioner said that there'd been no breaches of the database. Is that the understanding, Mr. George, Mr. Wilshusen—

Mr. GEORGE. That—

Mr. LIPINSKI. —your understanding?

Mr. GEORGE. That is our understanding, sir, yes, of their system itself—

Mr. LIPINSKI. Okay.

Mr. GEORGE. —of their hardware.

Mr. LIPINSKI. Do you have any—Mr. Wilshusen, any knowledge of—

Mr. WILSHUSEN. No, I do not have knowledge of specific incident. What I do know is that we identified a number of vulnerabilities that increase the risk of such an incident. But has one actually occurred on the databases I—we don't know of one yet.

Mr. LIPINSKI. Okay. And the Commissioner had talked about back in 2011, 2012 when these apps were being—online apps were being developed, that the NIST technical requirements were lower at that time. Now, first of all, is—Mr. George, is that your—because you had talked about them not meeting the requirements. Is that your understanding of how this happened?

Mr. GEORGE. It happened because of, again, the multifactor authentication versus the single-factor authentication. And the IRS took the approach that if they were to adopt the NIST standard of multifactor authentication, which would have included—in addition

to the basic information—utility bills and the like, that it would place an undue burden on taxpayers as they attempted to interact with the IRS. And while that is a laudable goal to make people's ability to comply with their taxes as easy as possible, it also had the detrimental effect of subjecting the IRS to vulnerabilities, which obviously manifested themselves with the IP PIN and with the Get Transcript application.

Mr. LIPINSKI. So, Commissioner, so was there a decision made to go forward with less cybersecurity, less security protection than the NIST requirements?

Mr. KOSKINEN. The NIST requirements start with, you know, you have to show up in person is their fourth level. The third level is you have to have multifactor authentication. The second level is other identification. And then the NIST process calls for them—there's no easy way to put everybody into one of those categories for a risk assessment to be made and the agency to decide at what level the risk is appropriately dealt with. As we said earlier, if you're making an online payment, that's a different risk issue.

When the system was developed, the determine—the review and a determination was made that a standard used for authentication, short of multifactor in the 2011 and '12 area, was use of out-of-wallet questions in addition to other identifiers. And in light of that and in light of the effectiveness of the system, it was determined that that would be an appropriate way to proceed pursuant to the NIST standards.

And I would note in the last filing season 7 million people downloaded 23 million legitimate transcripts. So——

Mr. LIPINSKI. Well, I want to—well, Mr. George had said that a risk assessment was not done for IP PIN. Is that correct, Mr. George? Is that——

Mr. GEORGE. A risk assessment was not done to the extent that it should have been is—and that——

Mr. LIPINSKI. Okay.

Mr. GEORGE. —and what I was really referring to was that a risk assessment was done for the Get Transcript, and they made the wrong call. They—that's what I stated earlier——

Mr. LIPINSKI. Okay.

Mr. GEORGE. —in my testimony. But they made—they considered——

Mr. LIPINSKI. The risk assessment——

Mr. GEORGE. —a very low risk——

Mr. LIPINSKI. —in your opinion, it seems like, from experience, was not——

Mr. GEORGE. They made the wrong call.

Mr. LIPINSKI. —was—okay. I'll just use your words. They made the wrong call. But there was a—so it wasn't just a—because back in 2011, 2012 that NIST wasn't saying you should have more. Obviously, after that and when this was in place NIST was saying there should be higher requirements if this needs level 3, if this reaches level 3, and it would seem that it would because of the, you know—the type of information that's at risk here. But the decision was made by the IRS to—because of the inconvenience, that that wouldn't be required.

Now, is there a different opinion now moving forward on this? And I think this is important not just for the IRS but across federal agencies about having a risk assessment that, you know, seems to be obviously in hindsight certainly and maybe in foresight it should have an obvious that there should have been a level 3 situation.

Mr. KOSKINEN. No, I think it's important, one of the things we've done over the last 2-1/2 years since I've been there is set up an enterprise-wide risk assessment program because the point is exactly what's happened here. You may make a risk decision and an assessment on any risk at a given point in time. The question is you need to continue to review that at least annually to see have the circumstances changed? Has the nature of the risk changed? Has the risk-reward ratio changed?

To say we made a judgment that IG thought we made—should have made a different judgment, but hindsight is always the question of whether, you know—if we knew then what we know now, we'd do a whole lot of things different. The real question is, and I think we have a process now to do that, is on a regular basis you should always review your risk assessments because the circumstances will change. And clearly in cybersecurity with the vast amount of personal data out there, the level of authentication you need today is significantly different than you would have needed four or five years ago.

Mr. LIPINSKI. Mr. George?

Mr. GEORGE. And just to clarify my statement a moment ago, Congressman, the IRS did not complete an authentication risk assessment for the identity—personal identification number, the identity protection personal identification number. And again, it was their thinking that it would be very burdensome on taxpayers had they done so and implemented a process as a result of that.

Mr. LIPINSKI. But I think sort of the bottom line of this part right here, not just for the IRS but for all departments, agencies across federal government is to do a good risk assessment and to continue to consider that—reconsider that and where it's been as things move very quickly. And I think it's very important that that does occur everywhere as we move forward.

So thank you. I yield back.

Mr. HULTGREN. [Presiding] The gentleman from Illinois yields back.

Chairwoman Comstock apologizes. She had a commitment in Transportation Committee that she had to run to, but I will yield myself five minutes for questions.

Just to follow up on Mr. Lipinski's question, Mr. George, if the IG says that even at the lower risk level the IRS process is not NIST-compliant, is that correct?

Mr. GEORGE. Repeat your question.

Mr. HULTGREN. If the IG says that—yes, so if you say that at the lower risk level the IRS process is not NIST-compliant, is that what you're saying?

Mr. GEORGE. It is—correct, because they would not require the additional information that NIST requested or mandated.

Mr. HULTGREN. Okay. Let me get to some of my other questions. First, I do want to thank you all for being here. The federal government certainly does have a massive cybersecurity problem, as we've

seen most visibly with the OPM data breach. We need to be doing more across the board to prevent, identify, and thwart cybersecurity attacks.

I had the opportunity to visit the Department of Energy's Cybersecurity Team at Germantown to get a crash course on the bad actors that exist. I also saw how easily a company or agency can find itself vulnerable. NIST develops the guidelines that all federal non-defense agencies must follow. For industry, they are minimal, a voluntary floor for our security. And it seems to me, however, that an agency can just ignore these rules, placing massive amounts of sensitive private information of my constituents at risk.

Mr. Koskinen, if I can address this to you. In regular business someone is usually responsible to accomplish their task and are held responsible for their failure to do so. IRS unfortunately has an abysmal record in holding their officials accountable, as we saw with the Lois Lerner incident a few years back. If you don't get fired for discriminating against political organizations and destroying evidence, I don't know how you would ever get fired at the IRS.

Mr. Wilshusen spoke about the enforcement actions that the federal government and said that he does not know that OMB has ever taken any action.

I appreciate your seemingly lamenting statement about the burden of mandates such as ObamaCare that they have on your agency, but all agencies have been strapped. And I think keeping my constituents' private information safe should be one of the highest priorities you have.

What internal actions have you taken considering you are still noncompliant with basic NIST and OMB standards?

Mr. KOSKINEN. I think we are compliant with NIST standards, as the Inspector General said. The prior authentication systems are no longer appropriate, and we agree with that and have taken those down. And in fact, with regard to go back in history about what happened in the past, the entire chain of command in the (c)(4) issues with regard to social welfare organizations is shortly thereafter—none of them were in place at the IRS. And so I don't think you can say people didn't leave, were not held accountable.

But I do think it is important for people to be accountable. I am actually talking to another Congressman now. We have any number of people who are in fact dismissed every year. For instance, we dismiss automatically anyone who uses improper access to any taxpayer information, any IRS employee. We discipline employees for being in default on their taxes. We have the highest compliance rate of any federal agency by a long shot, but even then, we take that very seriously. So I think it's not fair to imply that in fact people are not held accountable.

In cybersecurity we are dealing with a rapidly changing circumstance fighting increasingly organized and sophisticated criminal elements around the world. We are—as you say, we regret that we've had the difficulties we've had. We've had significant successes at the same time. We value the partnerships we have with the IG and the GAO and we're working to implement their security suggestions as quickly as we can.

Mr. HULTGREN. I would say in certainly the most high-profile situations we haven't seen that accountability and my constituents haven't, and they still are very fearful of their information.

Let me address—I just have a minute left—to Mr. George. In your prior testimony, Mr. Koskinen had stated that access to the “Get Transcript” application requires multistep authentication. Is multistep the same as multifactor authentication? If not, what is the difference, and could the use of the term multistep be disingenuous as it might confuse people into thinking they are the same?

Mr. GEORGE. They're the same. They're the same so——

Mr. KOSKINEN. And if I said multistep, multifactor is the term of art, and that's what we're working toward.

Mr. HULTGREN. Okay. Well, again, thank you all for being here, appreciate your work. This is obviously an ongoing concern for our constituents. They're frightened, quite honestly, of what could happen and might happen if their information is compromised. So I want to thank you all for being here.

And I'll yield back the balance of my time and I will thank the witnesses for their testimony and the members for their questions. The record will remain open for two weeks for additional written comments and written questions from members.

The hearing is adjourned.

[Whereupon, at 11:51 a.m., the Subcommittee was adjourned.]

Appendix I

ANSWERS TO POST-HEARING QUESTIONS

ANSWERS TO POST-HEARING QUESTIONS

Responses by The Honorable John Koskinen,

**House Committee on Science, Space, and Technology
Subcommittee on Research and Technology Hearing on
“Can the IRS Protect Taxpayers’ Personal Information?” QFRs**

Chairwoman Barbara Comstock

1. According to a November 2015 TIGTA report, the IRS is developing an e-Authentication framework that, once completed, will require multifactor authentication “for all applications that warrant a high level of assurance.”¹

- a. The IRS already rated the “Get Transcript” as a low-risk application even though unauthorized access to the website yielded 724,000 taxpayers’ confidential information – what assurance can you provide that the IRS will review applications differently in the future? What would qualify as an application that warrants a “high level” of assurance?**

IRS response: The IRS complies with both internal policies and external federal guidelines as a central tenet of its identity assurance strategy. The IRS follows Office of Management & Budget (OMB) M-04-04, which states that all federal agencies must conduct an e-authentication risk assessment on those systems that remotely authenticate users over a network for purposes of e-government and commerce to determine the required level of authentication assurance for the information system. The IRS also works closely with organizations such as the National Institute of Standards and Technology (NIST) to ensure best practices are followed and solutions meet the appropriate guidelines, e.g. NIST SP 800-63-2 (outlined in more detail in question 2 below).

We have redesigned the authentication process to meet Level 3 assurance, which requires multi-factor remote authentication techniques and applies to web applications requiring “High confidence in the asserted identity’s validity.” We also raised the risk assessment level of the Get Transcript application from moderate to high to more accurately reflect the risk demonstrated during the previous unauthorized accesses.

The IRS has committed to develop new strategies to protect taxpayer information and has worked closely with the Department of Homeland Security (DHS) and MITRE to perform extensive penetration testing to ensure integrity of our cybersecurity posture, including authentication. There is also a dedicated IRS team focusing exclusively on a cross-functional, enterprise-wide capability to provide secure account access to taxpayers. The IRS plans to expand this new Secure Access capability to all applicable online applications applying the appropriate levels of assurance to each application as required by OMB and NIST guidelines. As we expand multi-factor authentication to our online tools, balancing taxpayer accessibility with security will be a key area of focus for the IRS.

- b. When will the e-Authentication framework be fully developed and functional?**

¹ <https://www.treasury.gov/tigta/auditreports/2016reports/201640007fr.pdf>

IRS response: The IRS is developing an enterprise Identity Assurance Strategy across taxpayer contact channels to ensure Secure Access meets the needs of the IRS and manages data to enable taxpayers to access services through a variety of channels (e.g., online, phone, in-person). Taxpayers can continue to access IRS services through traditional service channels as well, including retrieving their transcript by mail. The Identity Assurance Strategy includes updated e-Authentication, which is now available and in use in conjunction with the Get Transcript application. The IRS plans to complete the Identity Assurance Strategy across all other contact channels by the end of calendar year 2016, with full implementation of the strategy occurring over a period of several years.

2. During the hearing, Rep. Bruce Westerman asked you when and how the National Institute of Standards and Technology (NIST) first informed the IRS (around the time when the agency developed the e-Authentication framework) that a Taxpayer Identification Number (TIN) was an acceptable government identification number for the purpose of authentication. Your response was that “It was part of a general framework.”

However, in response to a question from the Committee about the use of the TIN for the purpose of authentication, NIST replied that “NIST guidance describes different types of tokens that provide varying levels of security. However, this guidance does not recommend the use of identification numbers, including the TIN, as authentication tokens.”

Can you please provide the NIST reference document and specifically identify the guideline that initially identified for the IRS that the use of the TIN was an acceptable government identification number for the purpose of authentication? Absent that, can you provide any records or documents from NIST informing the IRS that a TIN was acceptable for authentication purposes? Absent that, can you provide any IRS records that explain how a decision was reached that concluded a TIN was an acceptable government identification number for the purpose of authentication?

IRS response: Question 2 relates to the registration and identity proofing of applicants as a component of the authentication process. The narrative below provides in-depth answers to each of the questions within this context.

The IRS uses NIST Special Publication 800-63-2, Electronic Authentication Guideline, which was published in August 2013, to establish confidence in user identities electronically presented to an information system. The technical Guideline, and the predecessor version that was in effect when e-Authentication was designed and built, includes as an element of identity-proofing the possession of a valid current government identification to allow an individual person to remotely authenticate his/her identity. Since it is not possible for a person to present an actual government-issued ID through an online identification process, the user can only provide information on the government-issued ID, such as the government ID number. NIST SP 800-63-2 clearly identifies the need for a government-issued ID number for remote identity proofing and presents “driver’s license or passport” as examples of government-issued IDs. In listing these examples, NIST SP 800-63-2 does not specifically limit those government-issued IDs that are acceptable for this purpose. In light of the clear citation as examples, and the limited number

(two) that were provided in the guideline, this was not interpreted as an exhaustive list of government-issued IDs or ID numbers that were considered acceptable.

In 2009, the IRS met with NIST to determine if an SSN could be used to satisfy this identity resolution. As documented in the attached minutes (NIST_NotesI-14-09.pdf), a conclusion was reached that, due in part to the IRS relationship that exists with the Social Security Administration (SSA) and the definition of Taxpayer Identification Numbers (TIN) in 26 USC 6109, which, for individuals, is generally an SSN, this identifier would be sufficient. NIST agreed that for the IRS, when it comes to identity resolution over the Internet, an SSN is as useful as a driver's license or passport number, and more so given the practicalities available to the IRS. In addition, we have attached a recent confirmation email from NIST that they are still in agreement with the 2009 discussions on this topic. We have also included a recent white paper IRS developed in response to a TIGTA recommendation.

Finally, of significant importance here, is the fact that the SSN is not the sole form of information requested by the IRS to identify an individual through any of the online or in-person channels IRS provides to taxpayers. Since the IRS began providing online applications to taxpayers through to the present day, the SSN has been one component of the identity proofing process. Today, for the online channel, SSN is just part of a multi-step process that includes multifactor authentication for both identity verification and for authentication of returning users for login or sign in. The identity verification process, using NIST guidelines, also includes verifying financial information and verification of the registered cell phone number. This is then followed by use of a Short Message Service (SMS) or text messages for second factor of authentication, ultimately leading to increased confidence in the user's identity, ensuring that the taxpayer is verified before allowing access to applications requiring a higher level of authentication such as Get Transcript online.



3. In response to another question from Rep. Bruce Westerman, Mr. Russell George suggested that the number of taxpayers whose information was stolen is higher than the 724,000 figure because “if someone gets access to information under the Get Transcript application when it was up and running, they also have access to dependent information and spouse information, so that number could be exponentially higher in terms of potential victims of identity theft or some--any other taxpayer mischief.”

What is your response to Mr. George's comment – does the 724,000 figure include spouse and dependent information? If not, can you provide the Committee a revised number to reflect the additional victims?

IRS response: The 724,000 figure reflects the number of taxpayer identification numbers for which there was a potentially suspicious access of a transcript via e-Authentication. We notified

all taxpayers whose accounts were accessed or access was attempted. We then used the transcript of the primary taxpayer to identify any secondary taxpayers (such as spouses or dependents) present on that transcript. These secondary taxpayers are not included in the count of 724,000 referenced by the TIGTA. We then sent a letter to all adults shown on the accessed transcripts. In addition to the original 724,000 letters sent to primary SSNs, we sent 471,000 letters to the other individuals whose SSNs appeared on transcripts. In developing the notifications for the Get Transcript fraudulent access, we alerted letter recipients, "...the unauthorized access to your account may include access to other Social Security Numbers (SSN) listed on your tax returns..." We did not include minors in our letter mail outs; we consider this reasonable as return filers would know those included on their submissions.

4. There are approximately 724,000 taxpayers whose information was stolen from the "Get Transcript" incident, and an additional few hundred thousand whose accounts were targeted, but whose data were not accessed. Your testimony explains that the IRS is providing credit monitoring to the group that had their data stolen, but not to those whose accounts were targeted, even though they are in a vulnerable position since criminals appear to have accessed some of their personal information from other sources.

Why is the IRS not offering equal protection to all the people whose accounts were targeted?

IRS response: Providing an identity theft monitoring product (commonly referred to as credit monitoring) is a standard practice when an incident causes sensitive information in the IRS's possession to be compromised and the risk of identity theft is high. This is also standard practice in private industry when a data breach occurs. The common principle is that the organization that exposes the sensitive information offers the credit monitoring.

We offered both credit monitoring and an opportunity to opt in to receive an Identity Protection Personal Identification Number (IP PIN) to those taxpayers whose personal tax information was compromised by thieves accessing our Get Transcript application. The information these thieves used to pass our e-Authentication was obtained from sources outside of the IRS. However, the thieves obtained tax return and account information from an IRS system (Get Transcript). As a result, we provided taxpayers whose account information was obtained through access to Get Transcript with the credit monitoring.

The additional population referenced did not have any of their personal information exposed from IRS systems. It is not readily apparent that the thieves had any of their information beyond name and SSN since the authentication attempt failed. As a courtesy, we notified these taxpayers that their personal information was apparently being used by identity thieves in a failed attempt to gain more information. We also included these SSNs in our system checks and filters allowing our processing system to recognize the SSNs as being potentially compromised. We will apply a higher level of protection to any return filed under those numbers.

Responses by The Honorable J. Russell George

Responses to Questions for the Record

House Committee on Science, Space, and Technology
related to the April 14, 2016 Testimony on
Protecting Taxpayers' Personal Information

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

**Questions submitted by Rep. Barbara Comstock, Chairwoman, Subcommittee on
Research and Technology**

1. According to a November 2015 TIGTA report and your testimony, the IRS determined the "authentication risk associated with 'Get Transcript' was low both to the IRS and taxpayers. The IRS defines a low risk rating as one in which the likelihood of an imposter to obtain and use the information available on 'Get Transcript' is low. In addition, a low risk concludes that controls are in place to prevent, or at least, significantly impede, an imposter from accessing the information."

- a. Should the recent thefts of data from OPM and other hacks such as the Anthem Health Insurance breach have raised red flags at the IRS since much of this stolen information was detailed enough to enable circumvention of single-factor authentication processes?

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

- b. Knowing the information that is accessible through these applications, would you have approved a single factor authentication as your security control?

Based on the risks involved, we believe that the Get Transcript and Identity Protection Personal Identification Number applications should have required multifactor authentication that complied with Government information security standards.

2. According to the November 2015 TIGTA report, the IRS "has not established a Service-wide approach to managing its authentication needs." Why is that, and are the IRS' security controls weaker because of this inconsistent approach?

The IRS recognized that there was a lack of consistency in techniques it had employed for authentication. As such, in June 2014, the IRS Wage and Investment Division established the Authentication Group. The Group provides centralized oversight and facilitates decision making for the development and integration of all forms of authentication including frameworks, policies, and processes across the IRS. However, the Authentication Group is not organizationally aligned within the IRS to effect cross-functional change. Establishing a Service-wide approach to managing the IRS's authentication needs is needed to ensure recommendations and any changes to authentication policy needed Service-wide to prevent future data breaches are properly implemented and monitored now and in the future.

The existence of differing levels of authentication assurance among the various access methods increases the risk of unscrupulous individuals accessing and obtaining personal taxpayer information and/or defrauding the tax system. Unscrupulous individuals can identify the weakest points of authentication and exploit them to inappropriately gain access to tax account information.

Question submitted by Rep. Randy Hultgren (R-IL)

1. During the hearing, I asked you about the IRS Commissioner's reference in prior testimony to needing multistep authentication to access the "Get Transcript" application. I asked you if multistep authentication was the same as multifactor authentication, and you replied that "They're the same." However, the November 2015 TIGTA Report (Reference Number: 2016-40-007), explains that "While taxpayers may have to complete multiple steps to authenticate their identity, these steps do not meet the requirements for a multifactor authentication." Would you care to correct your response for the record?

Yes. The single-factor, multistep authentication process used by the IRS is not multifactor authentication. While taxpayers had to complete multiple steps to authenticate their identity, these steps did not meet the requirements for a multifactor authentication. For example, the IRS requested basic identifying information from individuals seeking access to the Get Transcript application and required individuals to successfully answer knowledge-based questions provided by a third-party credit reporting agency. The IRS also asked the individual attempting to access the Get Transcript application to provide an e-mail address to which the IRS sent a confirmation code. While the IRS sent a confirmation code to the individual, this process did not meet the requirements for multifactor authentication because the IRS did not send the confirmation code to the e-mail address in the taxpayer's record nor was it a confirmation code that served as a second authentication factor to prove an individual's identity.

Responses by Mr. Gregory Wilshusen

Enclosure

Questions for the record from the Honorable Barbara Comstock, Chairwoman of the Subcommittee on Research and Technology, Committee on Science, Space, and Technology

1. According to a November 2015 TIGTA report and Mr. George's testimony, the IRS determined the "authentication risk associated with 'Get Transcript' was low to both the IRS and taxpayers. The IRS defines a low risk rating as one in which the likelihood of an imposter to obtain and use the information available on 'Get Transcript' application is low. In addition, a low risk concludes that controls are in place to prevent, or at least significantly impede an imposter from accessing the information."

- (a) Should the recent thefts of data from OPM and other hacks such as the Anthem Health Insurance breach have raised red flags at the IRS since much of this stolen information was detailed enough to enable circumvention of single-factor authentication processes?

Although the Office of Personnel Management breach was publicly disclosed after the Get Transcript incident occurred, the data theft at Anthem Health Insurance (disclosed in February 2015) should have prompted IRS to consider the theft's implications for the service. Agencies have been advised of the need for re-assessing risk and associated controls of their information systems and information. For example, National Institute of Standards and Technology (NIST) Special Publication 800-39¹ notes the importance of monitoring changes to the environment when managing risk, providing the specific example of changes in the threat environment that reports new tactics, techniques, procedures, or increases in the technical capabilities of adversaries. In addition, NIST Special Publication 800-53² recommends that agencies update system risk assessments whenever there are significant changes to a system's operating environment, including the identification of new threats and vulnerabilities. In its December 2003 e-authentication guidance to agencies,³ the Office of Management and Budget (OMB) points out that the final step in determining the appropriate assurance level is to periodically reassess the information system to ensure that the identity authentication requirements continue to be valid.

The data thefts indicated that attackers with the resources and technical skill to successfully exploit information security weaknesses and exfiltrate large quantities of data from computer systems were targeting organizations with large databases of personal information. Although the motives of these attackers may not be known, the information they stole reportedly contained personally identifiable information on tens of millions of individuals. Because IRS (1) maintains large databases containing personal information on millions of individuals and (2) required knowledge of a taxpayer's personal information to successfully

¹National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, MD: March 2011). Also see, for example, *Guide for Conducting Risk Assessments*, SP 800-30, Revision 1 (Gaithersburg, MD: September 2012), and *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, MD: February 2010).

²National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, MD: April 2013).

³Office of Management and Budget, *M-04-04: E-authentication Guidance for Federal Agencies* (Washington, D.C.: Dec. 16, 2003).

Enclosure

pass a single-factor authentication process to access the Get Transcript web-based application, it would have been appropriate for IRS to reassess the information security risk associated with the use of a knowledge-based, single-factor authentication for the application.

(b) Knowing the information that is accessible through these applications, would you have approved a single factor authentication as your security control?

Based on requirements and evolving threats, multi-factor authentication⁴ may be more appropriate for the application. According to OMB guidance,⁵ a high level of confidence in the asserted identity's validity is needed when an authentication error results in a moderate potential impact of the unauthorized release of sensitive information, financial loss, criminal violations that may be subject to enforcement efforts, and limited long-term inconvenience to any party. According to NIST guidelines,⁶ multi-factor authentication is needed to provide a high level of confidence in the authentication process.

As stated in my testimony,⁷ IRS has reported that unauthorized third parties had gained access to taxpayer information from the online Get Transcript application; in total about 724,000 tax accounts had been inappropriately accessed. The information that can be viewed or obtained through the Get Transcript application includes tax return information, tax account information, record of account, and wage and income information.⁸ Access to this information can enable an identity thief to file a fraudulent tax return that more closely resembles a legitimate tax return making it more difficult for the IRS to detect, potentially leading to a serious financial loss and criminal violations subject to enforcement efforts. This crime burdens legitimate taxpayers because authenticating their identities is likely to delay the processing of their tax returns and refunds. Moreover, the victim's personally identifiable information may be used to commit other crimes. The online Get Transcript application has been unavailable since May 2015, potentially creating a limited long-term inconvenience to taxpayers seeking information about their tax accounts. Based on these factors, OMB guidance indicates that a high level of confidence in the validity of an asserted identity is needed, thereby requiring, according to NIST guidelines, a multi-factor authentication process.

⁴Multi-factor authentication is a characteristic of an authentication system or token that uses two or more of the following factors to achieve authentication: something you know, something you possess, and something you are.

⁵M-04-04.

⁶National Institute of Standards and Technology, *Electronic Authentication Guideline*, SP 800-63-2 (Gaithersburg, MD: August 2013).

⁷GAO, *Information Security: IRS Needs to Further Enhance Controls over Taxpayer and Financial Data*, GAO-16-590T (Washington, D.C.: April 14, 2016).

⁸Treasury Inspector General for Tax Administration, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed*, 2016-40-007 (Washington, D.C.: Nov. 19, 2015).

Appendix II

ADDITIONAL MATERIAL FOR THE RECORD

REPORT SUBMITTED BY SUBCOMMITTEE CHAIRWOMAN
BARBARA COMSTOCK

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



***Improved Tax Return Filing and Tax Account
Access Authentication Processes
and Procedures Are Needed***

November 19, 2015

Reference Number: 2016-40-007

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number / 202-622-6500

E-mail Address / TIGTACommunications@tigta.treas.gov

Website / <http://www.treasury.gov/tigta>



HIGHLIGHTS

IMPROVED TAX RETURN FILING AND TAX ACCOUNT ACCESS AUTHENTICATION PROCESSES AND PROCEDURES ARE NEEDED

Highlights

**Final Report issued on
November 19, 2015**

Highlights of Reference Number: 2016-40-007
to the Internal Revenue Service Deputy
Commissioner for Services and Enforcement.

IMPACT ON TAXPAYERS

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

WHY TIGTA DID THE AUDIT

Failure to adequately authenticate taxpayers filing a tax return and accessing tax account services can lead to identity theft. The increased availability of personal information warrants an assessment of the authentication risk across IRS services. TIGTA performed this audit to assess IRS efforts to authenticate individual taxpayers' identities at the time tax returns are filed and when services are provided.

WHAT TIGTA FOUND

Taxpayers continue to desire electronic products and services that enable them to interact and communicate with the IRS. However, the continued challenge in expanding its portfolio of electronic products and services is that the IRS must ensure that tax account-related information and services are provided only to individuals who are entitled to receive them.

Although the IRS recognizes the growing challenge it faces in establishing effective authentication processes and procedures, it has not established a Service-wide approach to managing its authentication needs. The IRS should establish a function that is optimally placed in the organization and provide it with the authority needed to ensure that authentication policies and procedures are consistent and comply with Government information security standards Service-wide.

The IRS recognizes the need to establish a Service-wide approach to managing its authentication needs and has established two groups that focus on taxpayer authentication. However, neither of these groups provides for cross-functional management, oversight, and continued evaluation of the IRS's existing authentication processes to ensure that they address current and future needs.

In addition, authentication methods used for current online services do not comply with Government Information Security Standards. For example, TIGTA analysis of the e-Authentication processes used to authenticate users of the IRS online Get Transcript and Identity Protection Personal Identification Number applications found that the authentication methods provide only single-factor authentication despite the Government standards requiring multifactor authentication for such high-risk applications. As a result, unscrupulous individuals have gained unauthorized access to tax account information.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Deputy Commissioner for Services and Enforcement develop a Service-wide strategy that establishes consistent oversight of all authentication needs across IRS functions and programs, ensure that the level of authentication risk for all current and future online applications accurately reflects the risk, and ensure that the authentication processes meet Government Information Security Standards. The IRS agreed to implement all three recommendations.



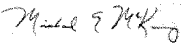
TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

November 19, 2015

**MEMORANDUM FOR DEPUTY COMMISSIONER FOR SERVICES AND
ENFORCEMENT**

FROM:


Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT:

Final Audit Report – Improved Tax Return Filing and Tax Account
Access Authentication Processes and Procedures Are Needed
(Audit # 201440016)

This report presents the results of our review to assess Internal Revenue Service efforts to authenticate individual taxpayers' identities at the time tax returns are filed and when obtaining services. This audit was included in our Fiscal Year 2015 Annual Audit Plan and addresses the major management challenge of Fraudulent Claims and Improper Payments.

Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have any questions, please contact me or Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services).



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

Table of Contents

Background	Page 1
Results of Review	Page 7
Authentication Processes and Procedures Do Not Provide Sufficient Assurance That Only Legitimate Individuals Are Filing Tax Returns and Accessing Tax Account Information	Page 7
A Service-Wide Strategy Is Needed to Ensure Consistent Oversight of Authentication Efforts	Page 10
<u>Recommendation 1:</u>	Page 13
Authentication Methods Used for Online Services Do Not Comply With Government Information Security Standards	Page 13
<u>Recommendation 2:</u>	Page 18
<u>Recommendation 3:</u>	Page 19
Appendices	
Appendix I – Detailed Objective, Scope, and Methodology	Page 20
Appendix II – Major Contributors to This Report	Page 22
Appendix III – Report Distribution List	Page 23
Appendix IV – List of Legislative Proposals for Congressional Consideration	Page 24
Appendix V – Management’s Response to the Draft Report	Page 26



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

Abbreviations

IP PIN	Identity Protection Personal Identification Number
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

Background

Taxpayers continue to desire electronic products and services that enable them to interact and communicate with the Internal Revenue Service (IRS). The IRS Oversight Board's¹ 2014 taxpayer attitude survey reported that 82 percent of taxpayers are likely to use a website, like the IRS public website (www.irs.gov), to help them comply with their tax obligations. In its most recent Strategic Plan,² the IRS acknowledged that the current technology environment has raised taxpayers' expectations for online customer service interactions and it needs to meet these expectations. In response, the IRS continues to expand the information and tools available online to assist taxpayers. The IRS's goal is to provide taxpayers with dynamic online account access that includes viewing their recent payments, making minor changes and adjustments to their accounts in real-time, and corresponding digitally with the IRS to respond to notices or complete required forms.

However, the continued challenge in expanding its portfolio of electronic products and services is that the IRS must ensure that tax account-related information and services are provided only to individuals who are entitled to receive them. For individuals seeking online services, authentication methods consist of three components:

- ***Identity Proofing*** – The process of collecting and verifying information about an individual for the purpose of issuing credentials, *i.e.*, a username and password, to that individual.
- ***Credential Issuance*** – Issuing an individual the tools needed to be authenticated by a system such as a user identification number and password.
- ***Authentication*** – The process of ensuring that the person requesting access is who they say they are by checking the credentials issued to the person after the identity proofing process.

For the purposes of this report, these three processes are collectively referred to as "authentication."

¹ The IRS Oversight Board is an independent body charged with overseeing the IRS in its administration, management, conduct, direction, and supervision of the execution and application of Internal Revenue laws. The Board was created to provide long-term focus and specific expertise in guiding the IRS so it may best serve the public and meet the needs of taxpayers.

² IRS Publication 3744, *Internal Revenue Service Strategic Plan – Fiscal Year 2014-2017*, pp. 6-7 (June 2014).



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

Office of Management and Budget (OMB) guidance *E-Authentication³ for Federal Agencies⁴* establishes criteria for determining the risk-based level of authentication assurance required for specific electronic applications and transactions. The guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. This guidance is intended to help agencies identify and analyze the risks associated with each step of the authentication process. As the outcome of an authentication error becomes more serious, the required level of assurance increases. The U.S. Department of Commerce National Institute of Standards and Technology (NIST)⁵ Special Publication 800-63-2, *Electronic Authentication Guideline*,⁶ provides the technical requirements for the four levels of assurance defined in OMB guidance. Figure 1 provides an overview of the technical requirements for the four NIST levels of e-Authentication assurance.

³ E-Authentication is the process of establishing confidence in user identities electronically presented to an information system.

⁴ OMB, M-04-04, *E-Authentication for Federal Agencies* (Dec. 2003).

⁵ The NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems.

⁶ NIST, NIST SP-800-63-2, *Electronic Authentication Guideline* (Aug. 2013).



**Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed**

Figure 1: Requirements for E-Authentication Levels of Assurance

Level of Assurance	Requirements	Level of Confidence
Level 1	No identity proofing is required.	Provides little or no confidence.
Level 2	Requires basic identity proofing data, ⁷ a valid current Government identification number, ⁸ and a valid financial or utility account number. ⁹ Access occurs only after identity proofing data and either the Government identification number or financial/utility account number are verified by the agency.	Provides some confidence in the validity of an individual's identity.
Level 3	Requires basic identity proofing data, a valid current Government identification number, and a valid financial or utility account number as well as the use of a second authentication factor such as a one-time supplemental code issued via text message or e-mail to the telephone number or e-mail address associated with the individual.	Provides high confidence in the validity of an individual's identity.
Level 4	Requires in-person identity proofing and verification.	Provides very high confidence in the validity of an individual's identity.

Source: NIST Special Publication 800-63-2 and OMB M-04-04.

IRS e-Authentication framework provides identity proofing for the applications included in the IRS's Service On Demand initiative

The IRS indicated that its e-Authentication framework once fully developed will enable the IRS to require multifactor authentication¹⁰ for all applications that warrant a high level of assurance. The IRS is developing and implementing the e-Authentication framework in four phases referred to as releases. Each release provides additional functionality. The current e-Authentication framework allows for only single-factor authentication.¹¹ Taxpayers desiring to access IRS online applications are first required to verify their identity through the e-Authentication framework. Figure 2 describes the current single-factor process the e-Authentication framework uses for first-time users of IRS online applications.

⁷ Name, address, date of birth, etc.

⁸ A driver's license number, passport number, etc.

⁹ A checking or savings account number, credit card account number, tax identification number, etc.

¹⁰ Multifactor authentication is a characteristic of an authentication system or a token that uses two or more authentication factors to achieve authentication. The three types of authentication factors are something you know, something you have, and something you are.

¹¹ Single-factor authentication is a characteristic of an authentication system or a token that uses one of three authentication factors to achieve authentication – something you know, something you have, and something you are.



**Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed**

**Figure 2: Current E-Authentication Framework
Single-Factor Identity Verification Process for First-Time Users**

Verification Steps	Description
E-Mail Confirmation	Individuals enter their first and last names and e-mail address. Prior to verifying their identity, the IRS sends a confirmation code to the e-mail provided by the individual. When they receive the code, they enter it into the appropriate field in the web page and continue with the identity verification process.
Identity Proofing (against IRS records)	The individuals enter their Taxpayer Identification Number (TIN), ¹² date of birth, filing status, and address from their most recently filed tax return. This information must match IRS records before the system allows them to go to the next step. If the information provided matches IRS records, they are given the option to create a user identification and password or proceed as a guest. ¹³ Guest access will require them to re-verify their identity every time they access the system.
Knowledge-Based Authentication	Individuals seeking access to Get Transcript and Identity Protection Personal Identification Number (IP PIN) applications are required to complete this step. Once individuals pass the match against IRS records, they must answer correctly a series of questions in order to further verify their identity. These are questions pulled from their credit report and other data sources via a third-party vendor.
Profile Creation and Credentials Issued (login with user identification and password)	Once a user profile is created, taxpayers will use their username and password to access the system in the future.

Source: Treasury Inspector General for Tax Administration (TIGTA) review of IRS documentation.

Establishing effective authentication processes is a Governmentwide challenge

The need to authenticate individuals requesting benefits and services is a Governmentwide challenge. A number of other Federal agencies have or are in the process of developing innovative processes in an effort to verify the identity of individuals seeking access to Federal benefits and services. For example:

- **Centers for Medicare and Medicaid Services Federal Healthcare Exchange** – Individuals wishing to use the Exchange will receive a username and password from the Exchange to create an online account at healthcare.gov prior to identity proofing. Individuals must provide name, date of birth, and residential address to complete identity proofing by going online to healthcare.gov or calling the Exchange. In order to submit an application,

¹² A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the TIN is an Employer Identification Number, a Social Security Number, or an Individual TIN.

¹³ Subsequent to the completion of our testing, the IRS eliminated the ability for taxpayers to obtain guest access.



**Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed**

receive an eligibility determination notice, and enroll and obtain insurance, individuals must correctly answer out-of-wallet¹⁴ questions provided by Experian Information Solutions, Inc. (an identity verifier).

Individuals who fail the online identity proofing session are instructed to call the Experian Verification Support Services Help Desk to validate their identity via the telephone. Individuals who are unable to have their identity validated by the Experian Verification Support Services Help Desk via telephone are offered other options to validate their identity such as manual authentication by mailing or uploading documentation.

- Department of Homeland Security myE-Verify application – Piloted in October 2014, *myE-Verify* allows individuals, using the Self-Lock feature, to lock their Social Security Number (SSN) so that no one else can use their SSN to get a job with an E-Verify employer,¹⁵ i.e., employment-related identity theft. To establish a *myE-Verify* account, an individual creates a username and password and passes an identity proofing quiz generated by an authentication service. The individual accesses their account using their username and password and also selects a communication channel they have access to for a second identity confirmation – a telephone call, text message, or e-mail message that contains a one-time passcode. As of April 2015, *myE-Verify* is available nationwide and will be available in Spanish in September 2015.
- Connect.Gov (formerly the Federal Cloud Credential Exchange) – *Connect.Gov* is a Governmentwide identity shared service run by the General Services Administration in partnership with the U.S. Postal Service. *Connect.Gov* allows the public to use a Government-approved, third-party digital credential to securely access online services at multiple agencies.
- General Services Administration MyUSA.gov – *MyUSA.gov* is a single-sign on option that will allow users to use one login to access websites from partner agencies and to provide a basic set of services through which agencies can interact with individuals. Individuals establishing an account on *MyUSA.gov* will provide their existing e-mail address and may also provide basic personal identifying information such as name, address, and telephone number. Individuals will not need a new password to log in. *MyUSA.gov* provides level one authentication assurance resulting in very little identity proofing. The benefit of *MyUSA.gov* is to provide individuals with a single access point for a large volume of low level account services. According to General Services Administration representatives, as of July 2015, *MyUSA.gov* and *Connect.Gov* product

¹⁴ Out-of-wallet questions refer to private information.

¹⁵ E-Verify is an Internet-based system that compares information from an employee's Form I-9, *Employment Eligibility Verification*, to data from U.S. Department of Homeland Security and Social Security Administration records to confirm employment eligibility.



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

efforts were merged to create a single identification authentication shared service for the Federal Government. The *MyUSA.gov* standalone functionality is no longer available to Federal agencies.

This review was performed at the IRS Wage and Investment Division Customer Account Services function in Atlanta, Georgia. In addition, we obtained information from the U.S. Department of Health and Human Services Centers for Medicaid and Medicare Services, the U.S. Department of Homeland Security, the U.S. Postal Service, and the General Services Administration. This review was conducted during the period November 2014 through August 2015. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

Results of Review

Authentication Processes and Procedures Do Not Provide Sufficient Assurance That Only Legitimate Individuals Are Filing Tax Returns and Accessing Tax Account Information

Although the IRS recognizes the growing challenge it faces in establishing effective authentication processes and procedures, our review identified that the IRS has not established a Service-wide approach to managing its authentication needs. As a result, the level of authentication the IRS uses for its various services is not consistent. The IRS has a need to authenticate individuals' identities at two primary points of interaction—filing and processing a tax return, and providing account-related services. The IRS offers a number of methods for taxpayers to interact with the IRS, e.g., online, in person, telephone. Different access methods may require different authentication processes. The existence of differing levels of authentication assurance among the various access methods increases the risk of unscrupulous individuals accessing and obtaining personal taxpayer information and/or defrauding the tax system. Unscrupulous individuals can identify the weakest points of authentication and exploit them to inappropriately gain access to tax account information.

Efforts to authenticate individuals filing a tax return are limited to taxpayers affected by identity theft

The only method the IRS uses to attempt to authenticate the identity of the tax return filer, *i.e.*, to ensure that the individual filing the tax return is the legitimate taxpayer, when processing a tax return is through its IP PIN process. The IRS issues an IP PIN to confirmed victims of identity theft as well as to individuals who may be at a high risk for identity theft, e.g., stolen wallet, victim of a non-IRS data breach. Individuals are not issued an IP PIN until they successfully complete the IRS identity proofing processes.¹⁶ The presence of a valid IP PIN on the tax return tells the IRS that the legitimate taxpayer is filing the tax return. According to the IRS, it issued more than 1.5 million IP PINs as of May 2, 2015, for use in filing a tax return during the 2015 Filing Season.

We recently reported that the IRS continues to improve its ability to detect identity theft-related tax returns.¹⁷ However, these processes require a significant number of IRS resources to verify the identity of every potential identity theft victim. A more efficient way to prevent identity theft

¹⁶ An explanation of the IP PIN identity theft proofing processes is provided on page 8 of this report.

¹⁷ TIGTA, Ref. No. 2015-40-026, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft* (Apr. 2015).



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

from occurring would be to establish a process that verifies the identity of the tax return filer at the time the tax return is accepted for processing. It has been suggested that the IRS expand the IP PIN program to all taxpayers. However, before doing so, the IRS must ensure that the IP PIN program will provide sufficient assurance that the individual who is requesting the IP PIN is who he or she claims to be. The IRS's current use of single-factor authentication processes to obtain access to request an IP PIN or to access an issued IP PIN does not ensure that it is accessible only to the legitimate taxpayer.

Processes used to authenticate individuals requesting access to similar information do not provide a consistent level of authentication assurance

The IRS has developed several methods to authenticate the identity of individuals accessing IRS services. However, we found that the various authentication processes used to gain access to similar information provide differing levels of authentication. For example, the processes the IRS has established to authenticate confirmed victims of identity theft for the purposes of issuing an IP PIN provide varying degrees of authentication assurance depending on how the IP PIN is obtained.

- The IRS directs identity theft victims whose Federal tax records have been affected to complete Form 14039, *Identity Theft Affidavit*, and submit it, by mail or fax, to the IRS along with a photocopy of at least one of four valid Federal or State Government-issued identification, *i.e.*, passport, driver's license, Social Security card, or other valid Federal or State-issued identification, to verify their identity. Once the IRS has verified an individual's identity, the IRS will send the individual a letter with the issued IP PIN for use in filing the next year's Federal tax returns.
- IRS confirmed victims of tax-related identity theft as well as residents of Florida, Georgia, and the District of Columbia have the option of receiving an IP PIN immediately by going online to the IP PIN page and verifying their identity through the e-Authentication framework. However, individuals who are authenticated by the e-Authentication framework are required to provide only basic identifying information and answer knowledge-based questions which can be circumvented by unscrupulous individuals. These individuals do not have to provide a photocopy of a valid Federal or State Government-issued identification.

We identified similar inconsistencies in the level of assurance provided by the processes the IRS uses to authenticate individuals requesting a tax account transcript. Figure 3 describes some of the most common services the IRS offers that require individuals to authenticate their identity before the requested service is provided.



**Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed**

Figure 3: IRS Services Requiring Authentication

Method of Access	Services Offered	Information Required for Authentication
IRS.gov and the e-Authentication Framework (Online Services)	Get Transcript – Provides a tax account or tax return transcript for a specific year.	TIN, name, date of birth, filing status, and mailing address from most recent tax return. Taxpayer also responds to personal questions, <i>i.e.</i> , prior addresses, car loan data, and mortgage information, generated from a third-party credit reporting company.
	IP PIN – Provides eligible taxpayers additional protection from the misuse of their SSN on fraudulent Federal income tax returns.	Taxpayer provided tax-related data are matched against data maintained on IRS databases. Personal questions are matched to information provided by a third-party credit reporting company.
	Online Payment Agreement – Provides individuals the ability to apply for an installment agreement.	
	Direct Pay – Provides individuals the option of paying their tax bill or making estimated tax payments directly from their checking or savings account.	
	Where's My Refund – Provides refund status information.	
Toll-Free Services	Tax Return, Tax Account Information, and Transcripts – Individuals can obtain assistance with tax account information and preparation of their tax returns. They can also obtain copies of their tax account transcripts by mail through an automated transcript telephone line.	TIN, first and last name, date of birth, and address. Taxpayer provided tax-related data are matched against data maintained on IRS databases. If information provided does not match, additional questions are asked to verify taxpayer identity.
	Tax Account Information – Individuals can obtain assistance in resolving tax account inquiries and adjustments.	Government-issued photo identification. If not available, taxpayer provides TIN, first and last name, date of birth, and address.
Walk-In Services (Taxpayer Assistance Centers)	Payments – Individuals can set up a payment plan and make payments on their tax account.	Taxpayer provided tax-related data are matched against data maintained on IRS databases. If information provided does not match, additional questions are asked to verify taxpayer identity.

Source: TIGTA's review of IRS documentation.

While OMB guidance and NIST standards apply to online interactions with individuals, both provide a solid framework that the IRS can use to consistently evaluate the level of



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

authentication assurance needed when accessing tax-related information. Once an appropriate level of assurance is determined for the tax information being accessed, the IRS can use these guidance and standards to ensure that all of the authentication processes it develops for accessing the same or similar information provide the needed level of assurance regardless of the access method or processes used.

A Service-Wide Strategy Is Needed to Ensure Consistent Oversight of Authentication Efforts

To effectively manage its authentication risk, the IRS should establish a function that is optimally placed in the organization and provide it with the authority needed to ensure that authentication policies and procedures are consistent and comply with Government information security standards Service-wide. The rising number of data breaches in the private and public sectors means that more personal information than ever is available to unscrupulous individuals. The increased availability of personal information necessitates an immediate and ongoing assessment of the authentication risk across the IRS. Appropriate steps to mitigate that risk should be taken to prevent unauthorized access and ensure consistency across all interactions with individuals. While the most reliable method of authenticating individuals is through face-to-face interaction, this method of authentication is burdensome for taxpayers and would require substantial IRS resources.

The IRS must look at all of its authentication and detection needs across IRS functional and program lines including its need to authenticate individuals who file tax returns as well as those who interact with the IRS face-to-face, over the Internet, or on the telephone. The IRS recognizes the need to establish a Service-wide approach to managing its authentication needs and has established two groups that focus on taxpayer authentication. However, neither of these groups provides for cross-functional management, oversight, and continued evaluation of the IRS's existing authentication processes to ensure that they address current and future needs.

The organizational placement of the Authentication Group limits its ability to fulfill its mission

The IRS recognized that there was a lack of consistency in techniques it had employed for authentication. As such, in June 2014, the IRS Wage and Investment Division established the Authentication Group. The Group provides centralized oversight and facilitates decision making for the development and integration of all forms of authentication including frameworks, policies, and processes across the IRS.

Since establishment, the Authentication Group has worked with various IRS functions with authentication responsibilities to improve its e-Authentication process. The Authentication Group has also assessed a number of initiatives including:



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

- Exploring the use of data analytics to strengthen its ability to authenticate individuals. The Group recognizes that the most effective method for combating identity theft is to use multiple methods to detect and prevent identity theft, including various layers of authentication in combination with detection processes.
- Using a third-party company to pilot face-to-face authentication in order to obtain an IP PIN. The third-party company approached the IRS about conducting the pilot. The Authentication Group provided oversight.
- Using a verification code for submitting Forms W-2, *Wage and Tax Statement*, that will be issued through secure e-mail to employers or payroll providers to enable the IRS to validate electronically submitted Forms W-2. This project was in the developmental stage prior to the formation of the Authentication Group.
- Assessing ways to improve e-Authentication by partnering with the IRS's contracted credit bureau agency to stop fraudsters and identity thieves from passing out-of-wallet questions.

While the Authentication Group is evaluating potential improvements to existing authentication methods for the purpose of preventing identity theft, it is not developing overall strategies to enhance authentication methods across IRS functions and programs. In addition, the Authentication Group is not evaluating new trends and schemes used to commit tax-related identity theft for the purpose of anticipating the IRS's future authentication needs. IRS management stated that it envisioned the Authentication Group would address the IRS's authentication needs Service-wide and acknowledged that while the Authentication Group has made progress, it is not yet achieving its mission.

The Authentication Group has not been provided with the authority to set Service-wide authentication policy

The Authentication Group is not organizationally aligned within the IRS to effect cross-functional change. The Group is part of the IRS Wage and Investment Division, yet other functions across the IRS are responsible for different aspects of taxpayer authentication. For example:

- The IRS's Cybersecurity function is responsible for setting security policy and all of the technology work related to the e-Authentication framework.
- The IRS's Privacy function is responsible for policy related to protecting taxpayer account information from disclosure.
- The Online Services function's role is to work with the IRS business divisions and Information Technology organization to develop web applications and the authentication framework.



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

The Authentication Group does meet regularly with these functions to identify potential changes to the authentication processes needed in the Wage and Investment Division's programs and services. However, other IRS functions outside of the Wage and Investment Division also have a need to authenticate taxpayers or their representatives which is not addressed by the Authentication Group. In addition, the group is unable to develop and integrate these processes into Service-wide authentication frameworks, policies, and processes.

In April 2015, the Authentication Group requested delegated authority¹⁸ from IRS executives to make limited changes to existing e-Authentication processes, as needed, based on analysis of e-Authentication usage data. IRS executives did not approve its request because they wanted to retain their authority to make authentication decisions.

The Security Summit Authentication Working Group was formed to identify both short-term and long-term solutions to combat identity theft

In March 2015, the IRS developed three working groups focused on combating tax-related identity theft across Federal, State, and private industry. The working groups include representatives from the IRS, State tax agencies, and the tax return preparation industry and are focused on three aspects of tax-related identity theft to find common areas of consensus and identify solutions.

- **Authentication Working Group** – This group was tasked with identifying opportunities for strengthening authentication practices, including identifying new ways to validate taxpayers and tax return information and new techniques for detecting and preventing identity theft refund fraud. The manager of the Wage and Investment Division's Authentication Group participated in this working group.
- **Information Sharing Working Group** – This group was tasked with identifying opportunities for sharing information that would improve the participants' capabilities for detecting and preventing identity theft refund fraud.
- **Strategic Threat Assessment and Response Group** – This group was tasked with taking a look across tax systems and best practices of other industries to identify points of vulnerabilities or risks and develop initiatives and solutions to detect and prevent identity theft refund fraud.

In June 2015, the IRS unveiled a multilayered approach to protect taxpayers from identity theft refund fraud across Federal and State tax systems and a series of recommendations covering six different areas for improvement for the 2016 Filing Season and beyond. These recommendations include efforts to authenticate taxpayers at the time Federal tax returns are filed and sharing of analytical data concerning fraud leads throughout the tax industry. Legislative proposals for Congressional consideration are listed in Appendix IV.

¹⁸ The assignment of responsibility or authority to carry out specific activities.



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

Establishing a Service-wide approach to managing the IRS's authentication needs is needed to ensure that the Security Summit's Authentication Working Group recommendations and any changes to authentication policy needed Service-wide to prevent future data breaches are properly implemented and monitored both currently and in the future.

Recommendation

The Deputy Commissioner for Services and Enforcement should:

Recommendation 1: Develop a Service-wide strategy that establishes consistent oversight of all authentication needs across IRS functions and programs including all interactions with individuals face-to-face, online, and through the telephone. In addition, the IRS should ensure that responsibility for implementing the strategy is optimally aligned to provide centralized oversight and facilitate decision making for the development and integration of all forms of authentication including frameworks, policies, and processes across the IRS.

Management's Response: The IRS agreed with this recommendation. The IRS has created a new position for an executive who will have responsibility for leading the development of this Service-wide strategy, and who will report to the Deputy Commissioner for Services and Enforcement to provide the necessary alignment and oversight of an integrated Service-wide approach.

***Authentication Methods Used for Online Services Do Not Comply
With Government Information Security Standards***

Although the IRS has established processes and procedures to authenticate some tax return filers and individuals requesting online access to IRS services, these processes and procedures do not comply with Government information security standards. In particular, the processes and procedures do not comply with the standards for assessing authentication risk and establishing adequate authentication processes. For example, our analysis of the e-Authentication processes used to authenticate users of the IRS online Get Transcript and IP PIN applications found that the authentication methods provide only single-factor authentication despite NIST standards requiring multifactor authentication for such high-risk applications. As a result, unscrupulous individuals have gained unauthorized access to tax account information.

OMB standards require Federal agencies to conduct an assessment of the risk of authentication error for each online service or application they provide. An authentication error occurs when an agency incorrectly confirms the identity provided by an individual when in fact the individual is not who he or she proclaims to be. In addition, NIST Special Publication 800-63 establishes specific requirements that agencies' authentication processes must meet to provide a specific level of authentication assurance.



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

For the IP PIN application, an authentication risk assessment was not completed as required

The IRS did not complete an authentication risk assessment of the IP PIN application as required. According to IRS management, a risk assessment was not completed for the IP PIN application because the e-Authentication framework will provide for multifactor authentication once completed. However, the IRS does not anticipate having the technology in place to provide multifactor authentication capability before the summer of 2016. Multifactor authentication requires the use of at least two authentication factors: 1) basic identifying information, knowledge-based questions, and financial-related questions; and 2) a second authentication factor such as a supplemental code that is provided only after the successful verification of the first authentication factor.

While IRS management recognized the IP PIN application required the use of multifactor authentication, they believed that requiring multifactor authentication would further burden identity theft victims who are attempting to obtain an IP PIN. As a result, the IRS decided to implement the online IP PIN application using the single-factor authentication processes currently available through the e-Authentication framework. Had the IRS conducted an authentication risk assessment for the IP PIN application, we believe it would have concluded that the risk to victims and the IRS of having their IP PINs compromised outweighed the potential burden.

For the Get Transcript application, the authentication risk assessment does not accurately reflect the risk of authentication error

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

Current single-factor, multistep authentication is not multifactor authentication

In testimony before the Senate Finance Committee on June 2, 2015, the IRS Commissioner testified that to access Get Transcript, taxpayers must go through a multistep authentication process to prove their identity. While taxpayers may have to complete multiple steps to authenticate their identity, these steps do not meet the requirements for a multifactor authentication. For example, the IRS requests basic identifying information from individuals seeking access to the Get Transcript application and requires individuals to successfully answer knowledge-based questions provided by a third-party credit reporting agency. The IRS also asks



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

the individual attempting to access the Get Transcript application to provide an e-mail address to which the IRS sends a confirmation code. While the IRS sends a confirmation code to the individual, this process does not meet the requirements for multifactor authentication because the IRS does not send the confirmation code to the e-mail address on the taxpayer's record nor is it a confirmation code that serves as a second authentication factor to prove an individual's identity (see Figure 2 on page 4).

While single-factor authentication provides some assurance that an individual attempting to access the online Get Transcript and IP PIN applications is the legitimate individual, the information typically required to authenticate an identity can be obtained from other sources. On May 14, 2015, IRS Computer Security Incident Response Center personnel identified a backlog of undeliverable e-mails. These e-mails were the confirmation code e-mails sent to Get Transcript users attempting to establish an account on the Get Transcript application. The IRS identified the undelivered e-mails being sent from suspicious sources. As a result of these unauthorized accesses, the IRS deactivated the Get Transcript application on May 21, 2015.

The IRS reported an estimated 615,000 unauthorized access attempts with an estimated 334,000 that were successful in using the information of victims to obtain a copy of their tax transcript. A successful access is one in which an unauthorized individual successfully answers identity proofing and knowledge-based authentication questions. The information that can be viewed or obtained through the Get Transcript application includes:

- **Tax return information** – available for the current and three prior years and includes most of the line items from a tax return as it was originally filed with the IRS.
- **Tax account information** – available for the current and nine prior years and includes basic account information including return type, marital status, adjusted gross income, taxable income, and payments made.
- **Record of account** – available for the current and three prior years and includes a combination of information from tax return and tax account information.
- **Wage and income** – available for the current and nine prior years and includes data from information returns reported to the IRS, such as Form W-2 and the Form 1099 series of information returns.
- **Verification of nonfiling** – available for the current and three prior years and includes proof from the IRS that the individual did not file a return for the year.

The IRS believes that some of this information may have been gathered to file fraudulent tax returns during the upcoming 2016 Filing Season. Access to this information can enable an identity thief to file a fraudulent tax return that more closely resembles a legitimate tax return making it more difficult for the IRS to detect. Based on these factors, the IRS should have rated the risk associated with the Get Transcript application as high, requiring a NIST level three multifactor authentication before access is granted. An additional concern is that individuals



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

who successfully create a user account and access the Get Transcript application do not have to re-authenticate their identity to gain access to the IP PIN application.

The IRS current single-factor authentication still does not meet NIST standards

It should be noted that the single-factor e-Authentication framework currently in use by the IRS does not meet NIST standards because it is unable to provide all of the functionality required by NIST standards for single-factor authentication. For example, NIST standards require agencies to obtain basic personal identifying information, a valid current Government identification number, *e.g.*, driver's license, passport number, and a financial or utility account number, *e.g.*, checking account; savings account; utility account; loan, credit card, or tax identification number. In addition, NIST standards also require agencies to confirm that the address, name, and date of birth associated with the Government identification number or financial/utility account number matches the information on the individual's application for access.

However, the IRS's current e-Authentication framework does not require individuals to provide Government identification or a financial or utility account number as required by NIST standards. According to IRS management, the IRS decided to not request financial or utility account information because the information cannot currently be verified. IRS management informed us that the IRS obtained and verified the taxpayer filing status to mitigate the risk of being unable to use financial information to authenticate individuals. Although the IRS required taxpayers to provide a filing status, this does not bring the IRS into compliance with NIST standards and the IRS remains noncompliant with single-factor authentication requirements.

The IRS requires individuals to provide their TIN as a form of Government identification. The IRS verifies the individual's name, date of birth, address, filing status, and TIN. The IRS received guidance from the NIST at the time the e-Authentication framework was being developed indicating that a TIN was an acceptable form of identification. However, in August 2015, the NIST informed us that a TIN is not currently an acceptable Government identification number for the purpose of authentication. We brought this discrepancy to the IRS's attention and IRS management agreed that a TIN is no longer an acceptable form of identification. Management also indicated the IRS would take steps to conform to NIST standards for verifying an individual's identity.

The availability of personal information to unscrupulous individuals increases the need for stronger authentication processes

The IRS's verification of knowledge-based questions in lieu of obtaining and verifying a valid Government identification and financial/utility account information does not make the IRS compliant with NIST standards for single-factor authentication. While the IRS cannot currently verify financial or utility account information, the requirement to obtain this information from individuals, regardless of whether it is verified, can serve as an added deterrent to discourage unscrupulous individuals from attempting to access tax information.



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

In addition, the requirement to provide financial information and a supplemental code for multifactor authentication is intended to make it more difficult for individuals who are not the legitimate taxpayer to bypass authentication processes. These added requirements can alert the valid taxpayer that someone is attempting to access their personal information, *i.e.*, when an unsolicited code is sent to them. Had the IRS required multifactor authentication, unscrupulous individuals may not have been able to access tax return information through the Get Transcript application.

Challenges exist in implementing the use of financial information and expanding to multifactor authentication

According to IRS management, the IRS will have the technical capability to use financial information to authenticate individuals as early as August 2015. The IRS anticipates it will have the technology to provide multifactor authentication as early as the summer of 2016. However, the IRS faces a number of challenges in being able to implement the use of financial information when authenticating individuals and expanding to multifactor authentication. For example, IRS management informed us that there are contractual issues related to the validation of financial data which need to be resolved before e-Authentication can be approved to operate at a higher level. In addition, once the technology to require financial information and multifactor authentication is available, the IRS still has to develop and implement the business processes needed to use financial information and multifactor authentication. For example, the IRS cannot efficiently and effectively provide a second factor of authentication, such as issuing a one-time code or token, to authenticate the individual's identity because it does not currently communicate with taxpayers via e-mail or text.

As a result, the use of multifactor authentication will require the IRS to send taxpayers the second authentication factor through the traditional mail, delaying access to needed services and negating the efficiency of using online services. The IRS is in the process of exploring secure methods to communicate with taxpayers through e-mail.

The IRS is pursuing a number of options to strengthen the online authentication processes

For more than a year, the IRS Authentication Group has been working collaboratively with functions across the IRS to identify options for strengthening the online authentication process provided by e-Authentication. As a result of the IRS's analysis of the Get Transcript event, the IRS has established controls to prevent concurrent attempts at authentication and increased its monitoring of repeated access attempts. The IRS has also blocked all identified questionable e-mail addresses and is planning to restrict access to one e-mail address per account registration. In addition, the IRS will now send a registration confirmation letter, *i.e.*, confirming the individual created a user account, to the taxpayer's address of record after a user profile has been created using the taxpayer's identity and will continue to do so after Get Transcript is



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

re-launched. As of July 21, 2015, the IRS had not established a target date for bringing the Get Transcript application back online.

IRS management informed us that the IRS is also evaluating additional options identified by the Authentication Group including a requirement for individuals to answer additional financial questions, requiring a credit card be linked to the user as an additional authentication factor, charging a nominal fee on a credit card for Get Transcript transactions as an additional authentication control, and sending an activation code via mail (and eventually e-mail and/or text message) to taxpayers' address of record after they pass identity proofing online and before allowing access to Get Transcript.

In considering these options, IRS management stated that they must balance strengthened authentication processes with ensuring that legitimate taxpayers are able to access services successfully without excessive burden. According to IRS management, the IRS is still in the process of finalizing its plans for strengthening its online authentication processes. IRS management stated that each new process the IRS implements will be tested and monitored to see how taxpayers respond and whether or not the desired result is being achieved.

Conclusion

No single authentication method or process will prevent unscrupulous individuals from filing identity theft tax returns or attempting to inappropriately access IRS services. However, strong authentication processes can reduce the risk of such activity by making it harder and more costly for unscrupulous individuals to gain access to resources and information. Therefore, it is important that the IRS ensure that its authentication processes are in compliance with NIST standards to provide the highest degree of assurance required and ensure that authentication processes used to verify individuals' identities are consistent among all methods used to access tax account information. NIST standards follow OMB guidance that require the level of authentication provided for electronic or online services be consistent with the risk to a Federal agency should an authentication error occur. Tax account information disclosed to unauthorized individuals can be used by identity thieves to prepare identity theft tax returns that more accurately reflect a valid return increasing the risk that fraudulent returns will not be detected by the IRS.

Recommendations

The Deputy Commissioner for Services and Enforcement should:

Recommendation 2: Ensure that the level of authentication risk for all current and future IRS online applications accurately reflects the risk to the IRS and taxpayers should an authentication error occur.

Management's Response: The IRS agreed with this recommendation. The IRS will review the e-Authentication risk assessment process to ensure that the level of



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

authentication risk for all current and future IRS online applications accurately reflects the risk to the IRS and taxpayers should an authentication error occur.

Recommendation 3: Ensure that the implemented authentication processes used for all current and future online applications provide the level of assurance required by NIST standards for the determined level of authentication risk.

Management's Response: The IRS agreed with this recommendation. The IRS will leverage NIST standards to ensure that implemented authentication processes used for all current and future online applications provide the required level of assurance for the determined level of authentication risk.



**Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed**

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess IRS efforts to authenticate individual taxpayers' identities at the time tax returns are filed and when obtaining services. To accomplish this objective, we:

- I. Identified and reviewed the methods and controls used by the IRS to authenticate taxpayers.
 - A. Researched IRS information, the Internal Revenue Manual, and interviewed IRS management and determined the processes in place to authenticate individuals' identity for both electronically filed returns and paper returns.
 - B. Determined the methods that the IRS uses to authenticate individuals using the *e-Authentication* program as well as taxpayers seeking tax account information using IRS toll-free telephone and walk-in services.
 - C. Evaluated the authentication processes the IRS is currently using and determined which processes resulted in the IRS verifying identities before a tax return is accepted for processing.
- II. Evaluated IRS plans to strengthen authentication procedures.
 - A. Obtained IRS plans to improve authentication controls used to prevent identity theft tax returns at the time of filing and other authentication controls currently in place. We interviewed IRS personnel, including those in the Wage and Investment Division Authentication Group, and identified authentication procedures being considered, developed, tested, or recently implemented.
 - B. Determined if taxpayers could obtain a Personal Identification Number from the IP PIN pilot program through the mail or by telephone.
 - C. Evaluated the current processes the IRS uses to authenticate taxpayers' identities before providing access to IRS services. We evaluated IRS plans to expand or strengthen existing processes used to verify the identity of taxpayers seeking services from the IRS, *i.e.*, *e-Authentication*, toll-free, walk-in services, as well as those processes used to electronically sign a tax return.
- III. Assessed methods used by States and Federal agencies to authenticate individuals.
 - A. Determined the authentication methods currently used and planned by interviewing representatives from selected States (Georgia, Indiana, Massachusetts, and the District of Columbia) and selected Federal agencies (Centers for Medicare and



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

- Medicaid Services Federal Healthcare Exchange, Department of Homeland Security, General Services Administration, and the *Connect.Gov* initiative).
- B. Met with representatives from organizations these State and Federal agencies work with (LexisNexis and Early Warning) and determined the services these organizations provide.
 - C. Evaluated the *Connect.Gov* program (formally the Federal Cloud Credential Exchange) used to authenticate individuals.
 - D. Evaluated the *myE-Verify* program used to authenticate individuals.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the IRS's methods and controls in place to authenticate taxpayers at the time tax returns are processed and when accessing IRS services and plans to strengthen authentication. We evaluated these controls by interviewing IRS management, reviewing current authentication methods, and reviewing authentication methods being developed.



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

Appendix II

Major Contributors to This Report

Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
Deann L. Baiza, Director
Bill R. Russell, Audit Manager
Wilma Figueroa, Lead Auditor
Sandra L. Hinton, Senior Auditor
Mark V. Willoughby, Senior Auditor
Kimberly Holloway, Auditor



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

Appendix III

Report Distribution List

Commissioner C
 Office of the Commissioner – Attn: Chief of Staff C
 Deputy Commissioner for Operations Support OS
 Commissioner, Wage and Investment Division SE:W
 Director, Office of Online Services SE:OLS
 Director, Customer Account Services, Wage and Investment Division SE:W:CAS
 Director, Privacy and Policy Compliance OS:P:PPC
 Director, Return Integrity and Compliance Services, Wage and Investment Division SE:W:RICS
 Director, Cybersecurity Operation OS:CTO:C:O
 Chief Counsel CC
 National Taxpayer Advocate TA
 Director, Office of Program Evaluation and Risk Analysis RAS:O
 Director, Office of Audit Coordination OS:PPAC:AC
 Office of Internal Control OS:CFO:CPIC:IC
 Audit Liaison: Chief, Program Evaluation and Improvement, Wage and Investment Division
 SE:W:S:PEI



**Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed**

Appendix IV

**List of Legislative Proposals
for Congressional Consideration**

In June 2015, the IRS *2015 Security Summit – Protecting Taxpayers from Identity Theft Refund Fraud* report identified the following six existing legislative proposals for congressional consideration to help fight against identify theft refund fraud:

- *Acceleration of information return (Forms W-2, Wage and Tax Statement, Form 1099 series of information returns, etc.) filing due dates* – Earlier receipt of information returns would enable the IRS to match wage and withholding information before releasing tax return refunds. The proposal would accelerate the filing due date for most information returns to January 31. Currently, most information returns are due by the last day of February after many taxpayers have already filed. As of March 6, 2015, the IRS had received more than 66.7 million tax returns.¹ This prohibits the IRS from effectively matching wage and withholding information prior to releasing tax return refunds.
- *Extending IRS authority to require truncated SSNs on Forms W-2* – Truncated SSNs on Forms W-2 would reduce the unnecessary risk of exposing SSNs to identity theft. Current legislation requires the inclusion of an employee's SSN on Forms W-2. The proposal would revise legislation to require employers to truncate the SSN by replacing the first five digits of the SSN with "x" or "*".
- *Expanded access to the Directory of New Hires* – The proposal would expand IRS access to the National Directory of New Hires database maintained by the Department of Health and Human Services. The database includes employment data and other valuable information for general tax administration purposes and would improve the IRS's ability to identify fraudulent returns at the time the return is processed.
- *Modifying criminal tax penalties for identity theft refund fraud* – The proposal would increase the maximum penalty from three years imprisonment and a \$100,000 fine to five years imprisonment and a \$250,000 fine. The proposal would also add a \$5,000 civil penalty (current law does not impose a civil penalty) on the individual who filed the fraudulent return and would be assessed immediately for each incidence of identity theft.
- *Correctable error authority* – The proposal would permit the IRS to adjust tax returns without performing an audit when the information provided by the taxpayer does not match the information contained in Government databases, the taxpayer has exceeded the

¹ TIGTA, Ref. No. 2015-40-032, *Interim Results of the 2015 Filing Season* p. 3 (Mar. 2015).



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

lifetime limit for claiming a deduction or credit, or the taxpayer has failed to include documentation with his or her return that is required by statute.

- *Authority to regulate tax return preparers* – Incompetent and dishonest paid tax return preparers potentially subject taxpayers to penalties and interest as a result of incorrect returns and undermine confidence in the tax system. The proposal to regulate paid tax return preparers is designed to promote high quality services, improve voluntary compliance, and foster taxpayer confidence in the fairness of the tax system.



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

Appendix V

Management's Response to the Draft Report



COMMISSIONER
WAGE AND INVESTMENT DIVISION

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

NOV 03 2015

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Debra Holland *Debra Z. Holland*
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – Improved Tax Return Filing and Tax
Account Access Authentication Processes and Procedures Are
Needed (Audit # 201440016)

Thank you for the opportunity to review and comment on the subject draft report. We appreciate your insight on authentication, and as you will see reflected in the attachment, we agree with all of your recommendations and are taking actions to implement them. We also appreciate the information you shared with regard to the efforts of other federal agencies to authenticate identities in their online environments. We reviewed this information and are continuing to work with other federal agencies to identify best practices, leverage information, and identify broader solutions.

As the demand for IRS services increases and resources have diminished, we have been focused on developing strategies to further improve taxpayer service. While we already actively engage with taxpayers across numerous communication channels, we are working diligently to meet taxpayers' increasing demands by expanding the range of self-service options, especially through lower-cost, higher-volume online channels. These options require significant investment to transform our services to secure digital interfaces, while simultaneously strengthening our cybersecurity efforts and expanding identity theft (IDT) work and related activities.

Securing our systems and protecting taxpayers' information is a top priority for the IRS. As criminals become more proficient at obtaining personal taxpayer information, authentication protocols need to be more sophisticated, moving beyond information that used to be known only to individuals, but now in many cases, is readily available to criminal organizations from various sources. We must balance the strongest possible authentication processes with the ability of taxpayers to legitimately access their data and use IRS services online.



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

2

In recognition of the critical importance of having a strong, coordinated and evolving authentication framework across the IRS, we have recently created a new position that is tasked with the responsibility for developing our Service-wide approach to authentication. Rene Schwartzman, an executive with almost 30 years of experience, has been chosen for this role, and she will have responsibility to and authority from the Deputy Commissioner for Services and Enforcement (DCSE) on this initiative.

In addition, we have engaged with the U.S. Digital Service (USDS), which uses the best of product design, engineering practices and technology professionals to build effective, efficient and secure digital channels to transform the way government works for the American people. We are joining forces with a team from USDS as we develop the future taxpayer digital experience and the foundational authentication standards that will enable secure digital exchanges between IRS and taxpayers. Rene has been tasked as the IRS lead for this effort, and she will be serving in this critical capacity on behalf of the entire enterprise, keeping the IRS Digital Subcommittee, DCSE and Commissioner apprised about the direction, status and progress of this effort on a regular basis.

To improve our efforts to fight against threats to the entire tax system by criminals who are able to undermine and circumvent authentication protocols, the Commissioner convened a security summit in March with leaders of the electronic tax industry, the software industry and State tax administrators. The group formed a public-private partnership committed to, among other things, working together to fortify authentication defenses and protocols across the board to protect taxpayers and thwart the criminals' access. The effort culminated in several recommendations for the upcoming filing season, which will strengthen authentication at time of filing. The IRS executive tasked with leading this cross-functional effort reports to the Commissioner and the DCSE on this important initiative. The partnership has expanded and is continuing its robust collaboration, because issues such as identity proofing and authentication are never-ending challenges that compel continuous evaluation, since identity thieves have proven to be resourceful and creative in compromising even the best multi-layered controls designed to protect against infiltration.

As noted above, we agree with your recommendations and are taking actions to implement them. We note, however, that we do not agree that the existence of differing levels of authentication assurance among the various access methods increases the risk of unscrupulous individuals accessing and obtaining personal taxpayer information. The National Institute of Standards and Technology (NIST) standards anticipate and require varying levels of assurance depending on the nature of the transaction and the information being exchanged. In addition, there are strong assurance processes easily available in some channels, but not others. For instance, in our Taxpayer Assistance Centers, IRS employees are able to verify the identity of taxpayers with photo identification, which provides a strong degree of authentication assurance; however, that method would not be feasible via Web and telephone interactions. Therefore, both the nature of the service channel and the service need drive variation in authentication



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

3

methods. Inconsistencies in the authentication methods/channels lead to favorable results. These inconsistencies actually strengthen authentication and, conversely, forced consistency could weaken it.

We appreciate the audit team accepting the guidance we provided from NIST showing that a Taxpayer Identification Number (TIN) was an acceptable form of identification at the time the e-Authentication framework was being developed. We relied on this guidance at the time of our initial decision regarding use of the TIN as government identification, but have recently learned that the NIST opinion on this matter has changed. Going forward, we will adjust our authentication protocols accordingly. Indeed, the realities of today's cybercriminals and identity thieves – who are constantly evolving, growing in sophistication and increasing their warehousing of stolen personal information – will require us to continually reassess and recalibrate our authentication protocols.

Attached are our comments to your recommendations. If you have any questions, please contact me, or a member of your staff may contact Ivy McChesney, Director, Customer Account Services, Wage and Investment Division, at (404) 338-8910.

Attachment



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

Attachment

Recommendation:

The Deputy Commissioner for Services and Enforcement should:

RECOMMENDATION 1

Develop a Service-wide strategy that establishes consistent oversight of all authentication needs across IRS functions and programs including all interactions with individuals face-to-face, online, and through the telephone. In addition, the IRS should ensure that responsibility for implementing the strategy is optimally aligned so as to provide centralized oversight and facilitate decision making for the development and integration of all forms of authentication including frameworks, policies, and processes across the IRS.

CORRECTIVE ACTION

We agree with this recommendation, and have created a new position for an executive who will have responsibility for leading the development of this service-wide strategy, and who will report to the DCSE to provide the necessary alignment and oversight of an integrated Service-wide approach.

IMPLEMENTATION DATE

Implemented

RESPONSIBLE OFFICIAL

Deputy Commissioner for Services and Enforcement

CORRECTIVE ACTION MONITORING PLAN

N/A

Recommendations:

The Deputy Commissioner for Services and Enforcement should:

RECOMMENDATION 2

Ensure that the level of authentication risk for all current and future IRS online applications accurately reflects the risk to the IRS and taxpayers should an authentication error occur.

CORRECTIVE ACTION

We agree with this recommendation and will review the e-Authentication risk assessment process to ensure that the level of authentication risk for all current and future IRS online applications accurately reflects the risk to the IRS and taxpayers should an authentication error occur.



***Improved Tax Return Filing and Tax Account Access
Authentication Processes and Procedures Are Needed***

2

IMPLEMENTATION DATE

December 15, 2016

RESPONSIBLE OFFICIAL

Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN

We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 3

Ensure that the implemented authentication processes used for all current and future online applications provide the level of assurance required by the NIST standards for the determined level of authentication risk.

CORRECTIVE ACTION

We agree with this recommendation and will leverage National Institute of Standards and Technology standards to ensure implemented authentication processes used for all current and future online applications provide the required level of assurance for the determined level of authentication risk.

IMPLEMENTATION DATE

December 15, 2015

RESPONSIBLE OFFICIAL

Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN

We will monitor this corrective action as part of our internal management control system.

REPORT SUBMITTED BY SUBCOMMITTEE CHAIRWOMAN
BARBARA COMSTOCK



United States Government Accountability Office

Report to Congressional Committees

September 2015

FEDERAL INFORMATION SECURITY

Agencies Need to Correct Weaknesses and Fully Implement Security Programs

GAO Highlights

Highlights of GAO-15-714, a report to congressional committees

Why GAO Did This Study

Since 1997, GAO has designated federal information security as a government-wide high risk area, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. In February 2015, in its high risk update, GAO further expanded this area to include protecting the privacy of personal information that is collected, maintained, and shared by both federal and nonfederal entities.

FISMA required federal agencies to develop, document, and implement an agency-wide information security program. The act also assigned OMB with overseeing agencies' implementation of security requirements.

FISMA also included a provision for GAO to periodically report to Congress on (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) agencies' implementation of FISMA requirements. GAO analyzed information security-related reports and data from 24 federal agencies, their inspectors general, and OMB; reviewed prior GAO work; examined documents from OMB and DHS; and spoke to agency officials.

What GAO Recommends

GAO is recommending that OMB, in consultation with DHS and others, enhance security program reporting guidance to inspectors general so that the ratings of agency security performance will be consistent and comparable. OMB generally concurred with our recommendation.

View GAO-15-714. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshusen@gao.gov.

September 2015

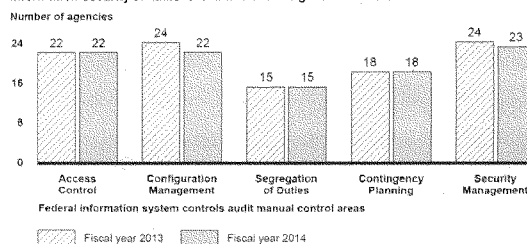
FEDERAL INFORMATION SECURITY

Agencies Need to Correct Weaknesses and Fully Implement Security Programs

What GAO Found

Persistent weaknesses at 24 federal agencies illustrate the challenges they face in effectively applying information security policies and practices. Most agencies continue to have weaknesses in (1) limiting, preventing, and detecting inappropriate access to computer resources; (2) managing the configuration of software and hardware; (3) segregating duties to ensure that a single individual does not have control over all key aspects of a computer-related operation; (4) planning for continuity of operations in the event of a disaster or disruption; and (5) implementing agency-wide security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks on an ongoing basis (see fig.). These deficiencies place critical information and information systems used to support the operations, assets, and personnel of federal agencies at risk, and can impair agencies' efforts to fully implement effective information security programs. In prior reports, GAO and inspectors general have made hundreds of recommendations to agencies to address deficiencies in their information security controls and weaknesses in their programs, but many of these recommendations remain unimplemented.

Information Security Weaknesses at 24 Federal Agencies in Fiscal Years 2013 and 2014



Source: GAO analysis of agency, inspectors general, and GAO reports issued by May 2015. (GAO-15-714)

Federal agencies' implementation in fiscal years 2013 and 2014 of requirements set by the *Federal Information Security Management Act of 2002* (FISMA) was mixed. For example, most agencies had developed and documented policies and procedures for managing risk, providing security training, and taking remedial actions, among other things. However, each agency's inspector general reported weaknesses in the processes used to implement FISMA requirements. In addition, to comply with FISMA's annual reporting requirements, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) provide guidance to the inspectors general on conducting and reporting agency evaluations. Nevertheless, GAO found that this guidance was not always complete, leading to inconsistent application by the inspectors general. For example, because it did not include criteria for making overall assessments, inspectors general inconsistently reported agency security performance.

Contents

Letter		1
	Background	4
	Continued Weaknesses Place Federal Agencies' Information and Information Systems at Risk	11
	Agencies' Implementation of FISMA 2002 Requirements Was Mixed	31
	Conclusions	54
	Recommendation for Executive Action	55
	Agency Comments and Our Evaluation	55
Appendix I	Objectives, Scope, and Methodology	57
Appendix II	Cyber Threats and Exploits	59
Appendix III	Number of Agency and Contractor-Operated Systems by Impact Level	62
Appendix IV	Comments from the Social Security Administration	63
Appendix V	GAO Contact and Staff Acknowledgments	64
Tables		
	Table 1: Critical Elements for Access Control to Computer Resources	19
	Table 2: National Cybersecurity Protection System Capabilities	26
	Table 3: Number of Agencies Documenting Information Security Policies and Procedures for Fiscal Years 2013 and 2014	34
	Table 4: Agency Incident Reporting and Response Practices as Reported for Fiscal Years 2013 and 2014	42
	Table 5: Total Number of Agency and Contractor-Operated Systems Reported for Fiscal Years 2013 and 2014 by Impact Level	45

Table 6: Reported Fiscal Year 2014 Federal Agencies Cybersecurity Spending by Major Category (amounts in millions)	48
Table 7: NIST FISMA-Related Publications	49
Table 8: Sources of Cybersecurity Threats	59
Table 9: Types of Cyber Exploits	60
Table 10: Cyber Events Characterized by Tactics, Techniques, and Practices	61
Table 11: Number of Agency and Contractor-Operated Systems in Fiscal Year 2014, by Impact Level	62

Figures

Figure 1: Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014	12
Figure 2: Information Security Incidents by Category, Fiscal Year 2014	13
Figure 3: Information Security Weaknesses at the 24 Agencies in Fiscal Years 2013 and 2014	18
Figure 4: Examples of Agencies' Implementation of Risk Management Program Elements Reported for Fiscal Years 2013 and 2014	32
Figure 5: Agencies' Implementation of Remediation Program Elements Reported for Fiscal Years 2013 and 2014	40
Figure 6: Agencies' Reported Cybersecurity Spending	47

Abbreviations

CAP	cross-agency priority
CDM	Continuous Diagnostics and Mitigation
CFO Act	<i>Chief Financial Officers Act of 1990</i>
CIO	chief information officer
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOT	Department of Transportation
Education	Department of Education
E-Gov Cyber	E-Gov Cyber and National Security Unit
EPA	Environmental Protection Agency
FedRAMP	Federal Risk and Authorization Management Program
FISCAM	<i>Federal Information System Controls Audit Manual</i>
FISMA 2002	<i>Federal Information Security Management Act of 2002</i>
FISMA 2014	<i>Federal Information Security Modernization Act of 2014</i>

GSA	General Services Administration
HHS	Department of Health and Human Services
HSPD-12	Homeland Security Presidential Directive 12
HUD	Department of Housing and Urban Development
NASA	National Aeronautics and Space Administration
NCPS	National Cybersecurity Protection System (EINSTEIN)
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	personally identifiable information
POA&M	plan of action and milestones
SBA	Small Business Administration
SSA	Social Security Administration
State	Department of State
TIC	Trusted Internet Connections
Treasury	Department of the Treasury
USAID	U.S. Agency for International Development.
US-CERT	United States Computer Emergency Readiness Team
USDA	U.S. Department of Agriculture
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

September 29, 2015

The Honorable Ron Johnson
Chairman
The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Jason Chaffetz
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The widespread use of the Internet has changed the way that our government, our nation, and the rest of the world communicate and conduct business. While the benefits have been enormous, this connectivity—without effective cybersecurity—can also pose significant risks to computer systems and networks as well as to the critical operations and key infrastructures they support. Resources may be lost, information—including sensitive personal information—may be compromised, and the operations of government and critical infrastructures¹ could be disrupted, with potentially catastrophic effects.

The emergence of increasingly sophisticated cyber threats underscores the need to manage and bolster the security of federal information systems. For example, advanced persistent threats—where an adversary that possesses sophisticated levels of expertise and significant resources can attack using multiple means such as cyber, physical, or deception to achieve its objectives—pose increasing risks. In addition, the number and

¹Critical infrastructure includes systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on national security. These critical infrastructures are chemical, commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors; materials; and waste, transportation systems; and water and wastewater systems.

types of cyber threats are on the rise. The recent attack on federal personnel and background investigation files that breached the personally identifiable information (PII)² for more than 20 million federal employees and contractors illustrates the need for strong security over information and systems. Further, in February 2015, the Director of National Intelligence testified³ that cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact.

Since 1997, we have designated federal information security as a government-wide high-risk area,⁴ and in 2003,⁵ expanded this area to include computerized systems supporting the nation's critical infrastructure. In our 2015 High-Risk update,⁶ we further expanded this area to include protecting the privacy of PII.

The *Federal Information Security Management Act of 2002* (FISMA 2002) established information security program and evaluation requirements for federal agencies in the executive branch.⁷ FISMA 2002 also assigned specific responsibilities to the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). Each year, each federal agency is to have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices. The results of the evaluation, performed by the agency's inspector general or independent external auditor, are to be reported annually to

²Personally identifiable information is information about an individual, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, or biometric records, and any other personal information that is linked or linkable to an individual.

³Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, testimony delivered on February 26, 2015.

⁴GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: February 2015).

⁵See GAO, *High-Risk Series: An Overview*, GAO/HR-97-1 (Washington, D.C.: February 1997) and *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

⁶See GAO-15-290.

⁷The *Federal Information Security Management Act of 2002* was enacted as Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946 (Dec. 17, 2002).

OMB, selected congressional committees, and the Comptroller General and are to address the adequacy of information security policies, procedures, practices, and compliance with requirements. The act also included a provision for GAO to periodically report to Congress on agency implementation of the act's provisions. FISMA 2002 was updated in 2014 by the *Federal Information Security Modernization Act of 2014*.⁸ Because FISMA 2002 requirements were in effect during the time period of our review, we are evaluating agencies' implementation of those requirements in this report. We will refer to the 2002 law as FISMA 2002 and the *Federal Information Security Modernization Act of 2014* as FISMA 2014. Changes in information security requirements under FISMA 2014 are discussed later in this section.

Our objectives were to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) federal agencies' implementation of FISMA 2002 requirements. To do this, we reviewed and analyzed the provisions of FISMA 2002 to identify responsibilities for implementing, overseeing, and providing guidance for agency information security. We also compared requirements for FISMA 2002 against those in FISMA 2014 to identify revised roles and responsibilities for OMB, the Department of Homeland Security (DHS), and federal agencies. We also analyzed our previous information security reports, annual agency FISMA reports, and agency financial and performance and accountability reports from the 24 federal agencies covered by the *Chief Financial Officers Act*,⁹ reports from the 24 agencies' Offices of Inspector General, OMB's annual reports to Congress on FISMA 2002 implementation, and NIST security publications issued for or during fiscal years 2013 and 2014. Where possible, we

⁸The *Federal Information Security Modernization Act of 2014* was enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), and amended chapter 35 of Title 44, U.S. Code. FISMA 2014 largely supersedes the very similar FISMA 2002 and expands the role and responsibilities of the Department of Homeland Security, but retains many of the requirements for federal agencies' information security programs previously set by the 2002 law.

⁹The 24 *Chief Financial Officers Act* agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and the U.S. Agency for International Development.

categorized findings from those reports according to information security program requirements prescribed by FISMA 2002 and security control areas defined by our *Federal Information System Controls Audit Manual*.¹⁰ We also reviewed OMB and DHS' annual FISMA reporting guidance and OMB's annual reports to Congress for fiscal years 2013 and 2014 FISMA implementation. In addition, we analyzed, categorized, and summarized the annual FISMA data submissions for fiscal years 2013 and 2014 by each agency's chief information officer, inspector general, and senior agency official for privacy.¹¹ We selected six agencies to determine the reliability of agency-submitted data. These agencies were selected to reflect a range in the number of systems agencies reported in fiscal year 2013 and include the Departments of Commerce, State, and Treasury; the General Services Administration; the National Science Foundation; and the Social Security Administration. While not generalizable to all agencies, the information we collected and analyzed provided insights into various processes in place to produce FISMA reports. We also conducted interviews with agency officials at OMB, DHS, NIST, and the six selected agencies. For the six agencies, we collected data from inspectors general and agency officials. Based on this assessment, we determined that the data were sufficiently reliable for our work.

We conducted this performance audit from December 2014 to September 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. For more details on our objectives, scope, and methodology, see appendix I.

Background

To help protect against threats to federal systems, FISMA 2002 set forth a comprehensive framework for ensuring the effectiveness of information

¹⁰GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

¹¹The inspectors general data submissions and OMB's report to Congress did not include information on recommendations that were made to address weaknesses discussed and any actions taken.

security controls over information resources that support federal operations and assets. This framework created a cycle of risk management activities necessary for an effective security program. It was also intended to provide a mechanism for improved oversight of federal agency information security programs. To ensure the implementation of this framework, FISMA 2002 assigned specific responsibilities to agencies, their inspectors general, OMB, and NIST.

FISMA 2002 required each agency in the executive branch to develop, document, and implement an information security program that includes the following components:

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- subordinate plans for providing adequate information security for networks, facilities, and systems or a group of information systems, as appropriate;
- security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and

-
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

In addition, each of the agencies in the executive branch were to report annually to OMB, certain congressional committees, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and their compliance with the act. FISMA 2002 also required each agency inspector general, or other independent auditor, to annually evaluate and report on the information security program and practices of the agency.

OMB's responsibilities included developing and overseeing the implementation of policies, principles, standards, and guidelines on information security in federal agencies except with regard to national security systems.¹² FISMA 2002 also assigned responsibility to OMB for ensuring the operation of a federal information security incident center. The required functions of this center are performed by DHS's United States Computer Emergency Readiness Team (US-CERT), which was established to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection. OMB is also responsible for reviewing, at least annually, and approving or disapproving agencies' information security programs.

Since it began issuing guidance to agencies in 2003, OMB has instructed agency chief information officers and inspectors general to report on a variety of metrics in order to satisfy reporting requirements established by FISMA 2002. Over time, these metrics have evolved to include administration priorities and baseline metrics meant to allow for measurement of agency progress in implementing information security-related priorities and controls. OMB requires agencies and inspectors

¹²As defined in FISMA 2002 and FISMA 2014, the term "national security system" means any information system used by or on behalf of a federal agency that (1) involves intelligence activities, national security-related cryptologic activities, command and control of military forces, or equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions (excluding systems used for routine administrative and business applications) or (2) is protected at all times by procedures established for handling classified national security information. See 44 U.S.C. § 3552(b)(6).

general to use an interactive data collection tool called CyberScope¹³ to respond to these metrics. The metrics are used by OMB to summarize agencies' progress in meeting FISMA 2002 requirements and report this progress to Congress in an annual report, as required by FISMA 2002.

NIST's responsibilities under FISMA 2002 included the development of security standards and guidelines for agencies that include standards for categorizing information and information systems according to ranges of impact-levels (See Federal Information Processing Standards 199 and 200),¹⁴ minimum security requirements for information and information systems in risk categories, guidelines for detection and handling of information security incidents, and guidelines for identifying an information system as a national security system.

During the 12 years FISMA 2002 was enacted into law and then largely replaced by FISMA 2014, executive branch oversight of agency information security has evolved. As part of its FISMA 2002 oversight responsibilities, OMB has issued annual instructions for agencies and inspectors general to meet FISMA 2002 reporting requirements. In July 2010, the Director of OMB and the White House Cybersecurity Coordinator issued a joint memorandum¹⁵ that gave DHS primary responsibility within the executive branch for the operational aspects of cybersecurity for federal information systems that fall within the scope of FISMA 2002. This memo stated that DHS would have these five responsibilities:

- overseeing implementation of and reporting on government cybersecurity policies and guidance;
- overseeing and assisting government efforts to provide adequate, risk-based, and cost-effective cybersecurity;

¹³CyberScope is an interactive data collection tool that has the capability to receive data feeds on a recurring basis to assess the security posture of a federal agency's information infrastructure. Agencies are required to use this tool to report metrics.

¹⁴NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004) and NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, Md.: March 2006).

¹⁵OMB, *Memorandum M-10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security* (Washington, D.C.: July 6, 2010).

-
- overseeing agencies' compliance with FISMA 2002;
 - overseeing agencies' cybersecurity operations and incident response; and
 - annually reviewing agencies' cybersecurity programs.

The OMB memo further stated that, in carrying out these responsibilities, DHS was to be subject to general OMB oversight in accordance with the provisions of FISMA 2002. In addition, the Cybersecurity Coordinator would lead the interagency process for cybersecurity strategy and policy development.

In accordance with guidance contained in the memo, DHS, instead of OMB, issued guidance to agencies and inspectors general on metrics used for reporting agency performance of cybersecurity activities and privacy requirements, while OMB continued to provide more general reporting guidance.¹⁶ Specifically, DHS provided guidance to agencies for reporting on the implementation of security requirements in areas such as continuous monitoring, configuration management, incident response, security training, and contingency planning, among others. The guidance also instructs inspectors general on reporting the results of their annual evaluations and instructs senior agency officials for privacy on reporting their agencies' implementation of privacy requirements.

As previously mentioned, DHS is also responsible for ensuring the operation of a federal information security incident center to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection. Within DHS, the Federal Network Resilience division's Cybersecurity Performance Management Branch is responsible for (1) developing and disseminating FISMA 2002 reporting metrics, (2) managing the CyberScope web-based application, and (3) collecting and reviewing federal agencies' cybersecurity data submissions and monthly data feeds to CyberScope. In addition, the Cybersecurity Assurance Program Branch is responsible for conducting cybersecurity reviews and

¹⁶Fiscal year 2013 reporting instructions for FISMA and agency privacy management were issued by DHS as *Federal Information Security Memorandum 13-01* (Sept. 4, 2013) and by OMB as M-14-04 (Nov. 18, 2013). Fiscal year 2014 reporting instructions were issued by DHS as *Federal Information Security Memorandum 14-01* (undated memo) and by OMB as M-15-01 (Oct. 3, 2014). The DHS and OMB memos vary in content.

New FISMA Requirements
Clarify Roles and
Responsibilities

assessments at federal agencies to evaluate the effectiveness of agencies' information security programs.

To further improve cybersecurity and clarify oversight responsibilities, Congress passed FISMA 2014.¹⁷ FISMA 2014 is intended to address the increasing sophistication of cybersecurity attacks, promote the use of automated security tools with the ability to continuously monitor and diagnose the security posture of federal agencies, and provide for improved oversight of federal agencies' information security programs. Specifically, the act clarifies and assigns additional responsibilities to OMB, DHS, and federal agencies in the executive branch. These new responsibilities include:

OMB responsibilities

- Preserves OMB's oversight responsibilities, but removes the requirement for OMB to annually review and approve agencies' information security programs.
- Requires OMB to include in its annual report to Congress a summary of major agency information security incidents, an assessment of agency compliance with NIST standards, and an assessment of agency compliance with breach notification requirements. For two years after enactment, OMB is to include in its annual report an assessment of agencies' adoption of continuous diagnostic technologies and other advanced security tools.
- Requires OMB to update data breach notification policies and guidelines periodically and require notice to congressional committees and affected individuals.
- Expands exemptions from OMB oversight for certain national security-related systems.
- States that OMB shall, in consultation with DHS, the Chief Information Officers Council, the Council of Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, ensure the

¹⁷Note: This report covers agencies' fiscal years 2013 and 2014 efforts under the requirements of FISMA 2002.

development of guidance for evaluating the effectiveness of an information security program and practices.

DHS responsibilities

- Establishes DHS responsibility, in consultation with OMB, to administer the implementation of agency information security policies and practices for information systems other than national security systems, the Department of Defense, and the Intelligence community's "debilitating impact" systems.
- Requires DHS to develop, issue, and oversee implementation of binding operational directives to agencies. Such directives include those for incident reporting, contents of annual agency reports, and other operational requirements.
- Gives DHS responsibility to operate the federal information security incident center, deploy technology to continuously diagnose and mitigate threats, compile and analyze data, and develop and conduct targeted operational evaluations, including threat and vulnerability assessments of systems.

Executive branch agency responsibilities

- Requires agencies to comply with DHS operational directives in addition to OMB policies and procedures and NIST standards.
- Requires agencies to ensure that senior officials carry out assigned responsibilities and that all personnel are held accountable for complying with the agency's information security program.
- Requires agencies to use automated tools in periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices.
- Requires agencies to report major security incidents to Congress within 7 days. Agencies are also to include a description of major incidents in their annual report to Congress.
- FISMA 2014 also requires that the annual independent evaluation include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. This replaces the previous FISMA 2002 requirement that the independent annual evaluation include an assessment of agency compliance with the

requirements of the act and related policies, procedures, standards, and guidelines.

In addition, FISMA 2014 reiterates the previous requirement for federal agencies to develop, document, and implement an agency-wide information security program. Each agency and its Office of Inspector General are still required to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of the agency's information security policies, procedures, practices, and compliance with requirements.

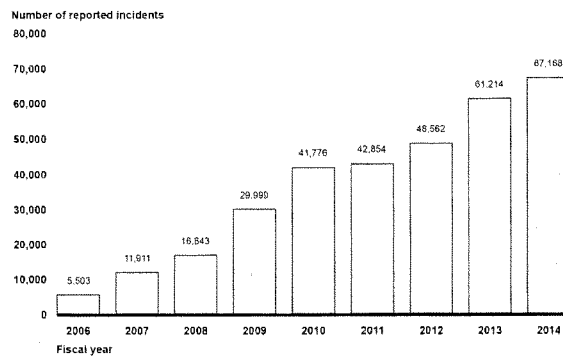
Continued Weaknesses Place Federal Agencies' Information and Information Systems at Risk

During fiscal years 2013 and 2014, federal agencies continued to experience weaknesses in protecting their information and information systems. These systems remain at risk as illustrated in part by the evolving array of cyber-based threats and the increasing numbers of incidents reported by federal agencies. (See app. II for additional information on cyber threats and exploits.) At the same time, weaknesses in their information security policies and practices hinder their efforts to protect against threats. Furthermore, our work and reviews by inspectors general highlight information security control deficiencies at agencies that expose information and information systems supporting federal operations and assets to elevated risk of unauthorized use, disclosure, modification, and disruption. Accordingly, we and agency inspectors general have made hundreds of recommendations to agencies to address these security control deficiencies.

Number of Incidents Reported by Federal Agencies Continues to Increase

The number of information security incidents affecting systems supporting the federal government has continued to increase. Since fiscal year 2006, the number rose from 5,503 to 67,168 in fiscal year 2014: an increase of 1,121 percent. Figure 1 illustrates the increasing number of security incidents at federal agencies from 2006 through 2014.

Figure 1: Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014



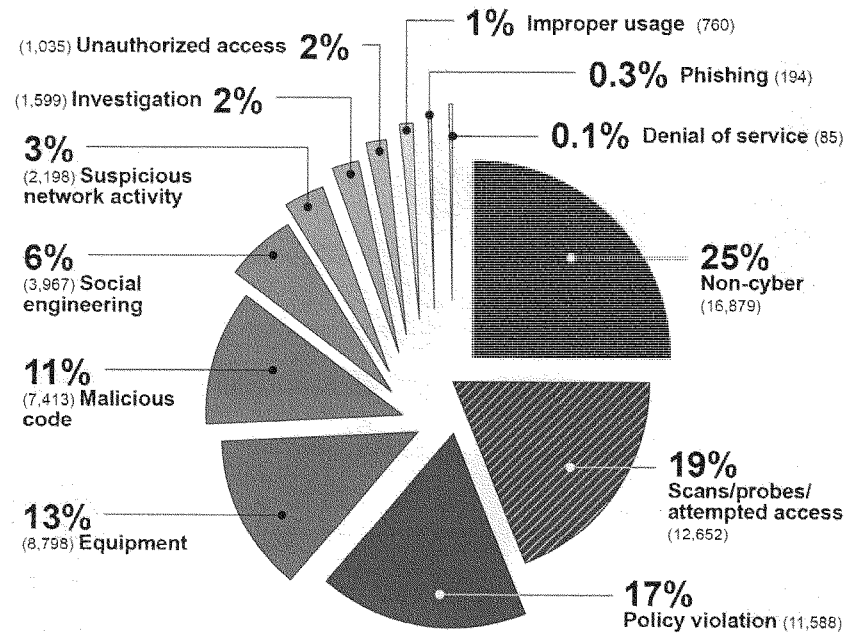
Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-714

Similarly, the number of information security incidents involving PII reported by federal agencies has more than doubled in recent years, from 10,481 in 2009 to 27,624 in 2014.

Of the incidents occurring in 2014 (not including those reported as non-cyber incidents)¹⁶ scans/probes/attempted access was the most widely reported type of incident across the federal government. This type of incident can involve identifying a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. As shown in figure 2, these incidents represented 19 percent of the various incidents reported to US-CERT in fiscal year 2014.

¹⁶A non-cyber incident is a report of PII spillage or possible mishandling of PII that involves hard copies or printed material as opposed to digital records.

Figure 2: Information Security Incidents by Category, Fiscal Year 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-15-714

These incidents and others like them can pose a serious challenge to economic, national, and personal privacy and security. Recent examples highlight the impact of such incidents:

- In June 2015, OPM reported that an intrusion into its systems affected the personnel records of about 4.2 million current and former federal employees. The Director of OPM also stated that a separate but

related incident affected background investigation files and compromised OPM systems related to background investigations for 21.5 million individuals.

- In June 2015, the Commissioner of the Internal Revenue Service testified that unauthorized third parties had gained access to taxpayer information from its "Get Transcript" application. According to officials, criminals used taxpayer-specific data acquired from non-department sources to gain unauthorized access to information on approximately 100,000 tax accounts. These data included Social Security information, dates of birth, and street addresses. In an August 2015 update, the Internal Revenue Service reported this number to be about 114,000, and that an additional 220,000 accounts had been inappropriately accessed, which brings the total to about 330,000 accounts.
- In April 2015, the Department of Veterans Affairs' Office of Inspector General reported that two contractors had improperly accessed the agency's network from foreign countries using personally owned equipment.¹⁹
- In February 2015, the Director of National Intelligence stated that unauthorized computer intrusions were detected in 2014 on the networks of the Office of Personnel Management and two of its contractors. The two contractors were involved in processing sensitive PII related to national security clearances for federal employees.²⁰
- In September 2014, a cyber intrusion into the United States Postal Service's information systems may have compromised PII for more than 800,000 of its employees.²¹

¹⁹Department of Veterans Affairs, Office of Inspector General, *Administrative Investigation Improper Access to the VA Network by VA Contractors from Foreign Countries Office of Information and Technology Austin, TX, Report No. 13-01730-159* (Washington, D.C.: April 2015).

²⁰James R. Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, testimony before the Senate Committee on Armed Services, Feb. 26, 2015.

²¹Randy S. Miskanic, Secure Digital Solutions Vice President of the United States Postal Service, *Examining Data Security at the United States Postal Service*, testimony before the Subcommittee on Federal Workforce, U.S. Postal Service and the Census, 113th Congress, Nov. 19, 2014.

-
- In October 2013, a wide-scale cybersecurity breach involving a U.S. Food and Drug Administration system occurred that exposed the PII of 14,000 user accounts.²²
-

**Cybersecurity Deficiencies
Continue to Place
Systems at Risk**

Our work at federal agencies continues to highlight information security deficiencies in both financial and nonfinancial systems. We have made hundreds of recommendations to agencies to address these security control deficiencies, but many have not yet been fully implemented. The following examples describe the risks we found at federal agencies, our recommendations, and the agencies' responses to our recommended actions.

- In March 2015, we reported that the Internal Revenue Service had not installed appropriate security updates on all of its databases and servers, and had not sufficiently monitored control activities that support its financial reporting and protect taxpayer data. Also, the agency had not effectively maintained secure settings or separation of duties by allowing a developer unnecessary access to a key application. In addition to 51 recommendations made in prior years that remain unimplemented, we made 19 additional recommendations to help the agency more effectively implement elements of its information security program and address newly identified control weaknesses. The Internal Revenue Service agreed to develop corrective action plans, as appropriate, to address these recommendations.²³
- In January 2015, we reported that the Federal Aviation Administration had significant security control weaknesses in the five air traffic control systems we reviewed. These systems perform functions such as determining and sharing precise aircraft location, streaming flight information to cockpits of aircraft, providing telecommunications infrastructure for NextGen, and are necessary for ensuring the safe and uninterrupted operation of the national airspace system. We identified numerous weaknesses in controls intended to prevent, limit,

²²Department of Health and Human Services, Office of Inspector General, *Penetration Test of the Food and Drug Administration's Computer Network*, Report No. A-18-13-30331 (Washington, D.C.: October 2014).

²³GAO, *Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data*, GAO-15-337 (Washington D.C.: March 19, 2015).

and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on its systems. The agency also had not fully implemented an agency-wide information security program, in part due to not having fully established an integrated, organization-wide approach to managing information security risk. We made 168 recommendations to the agency to mitigate control deficiencies and 17 recommendations to fully implement its information security program and establish an integrated approach to managing information security risk. The Federal Aviation Administration concurred with our recommendations, described actions that it was taking to improve its information security, and indicated that it would address the recommendations.²⁴

- In November 2014, we reported that the Department of Veterans Affairs had not taken effective actions to contain and eradicate a significant incident detected in 2012 involving a network intrusion. Further, the department's actions to address vulnerabilities identified in two key web applications were insufficient. Additionally, vulnerabilities identified in workstations (e.g., laptop computers) had not been corrected. We made eight recommendations to address identified weaknesses in incident response, web applications, and patch management. The department concurred with our recommendations and provided an action plan for addressing the identified weaknesses.²⁵

Similar to our work, independent reviews at the 24 agencies continued to highlight deficiencies in their implementation of information security policies and procedures. Specifically, for fiscal year 2014, 19 agencies reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls over their

²⁴GAO, *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*, GAO-15-221 (Washington D.C.: Jan. 29, 2015).

²⁵GAO, *Information Security: VA Needs to Address Identified Vulnerabilities*, GAO-15-117 (Washington D.C.: Nov. 13, 2014).

financial reporting.²⁶ This reflected an increase from fiscal year 2013, when 18 agencies reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls over their financial reporting. Further, 23 of 24 inspectors general for the agencies cited information security as a "major management challenge" for their agency, reflecting an increase from fiscal year 2013, when 21 inspectors general cited information security as a major challenge. The inspectors general made numerous recommendations to address these issues, as discussed later in this report.

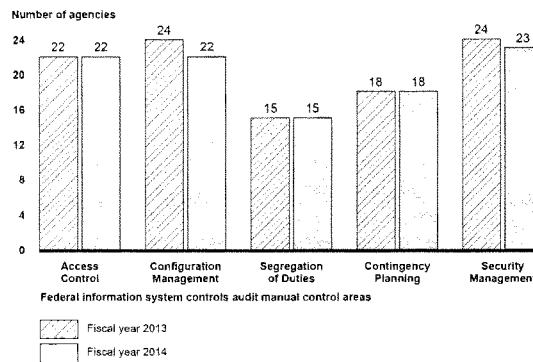
**Agencies Exhibited
Weaknesses in All Major
Categories of Controls**

Our reports, agency reports, and inspectors general assessments of information security controls during fiscal years 2013 and 2014 revealed that most of the 24 agencies had weaknesses in each of the five major categories of information system controls: (1) access controls, which limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure; (2) configuration management controls, intended to prevent unauthorized changes to information system resources (for example, software programs and hardware configurations) and assure that software is current and known vulnerabilities are patched; (3) segregation of duties, which prevents a single individual from controlling all critical stages of a process by splitting responsibilities between two or more organizational groups; (4) contingency planning, which helps avoid significant disruptions in computer-dependent operations; and (5) agencywide security management, which provides a framework for ensuring that risks are understood and that effective controls are selected, implemented, and operating as intended.

While the number of agencies exhibiting weaknesses decreased slightly in two of five categories, deficiencies were prevalent for the majority of them, as shown in figure 3.

²⁶A "material weakness" is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A "significant deficiency" is a control deficiency, or combination of control deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A "control deficiency" exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

Figure 3: Information Security Weaknesses at the 24 Agencies in Fiscal Years 2013 and 2014



Source: GAO analysis of agency, inspectors general, and GAO reports issued by May 2015. | GAO-15-714

In the following subsections, we discuss the specific information security weaknesses agencies reported for fiscal years 2013 and 2014.

Most Agencies Had Weaknesses in Access Controls

Agencies use electronic and physical controls to limit, prevent, or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized use, modification, disclosure, and loss. Access controls involve the six critical elements described in table 1.

Table 1: Critical Elements for Access Control to Computer Resources

Element	Description
Boundary protection	Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from devices that are connected to a network. For example, multiple firewalls can be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems, and intrusion detection and prevention technologies can be deployed to defend against attacks from the Internet.
User identification and authentication	A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns a unique user account to specific users, the system is able to distinguish one user from another—a process called identification. The system also must establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric). The combination of identification and authentication provides the basis for establishing accountability and for controlling access to the system.
Authorization	Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. For example, operating systems have some built-in authorization features such as permissions for files and folders. Network devices, such as routers, may have access control lists that can be used to authorize users who can access and perform certain actions on the device.
Cryptography	Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. Examples of cryptographic services are encryption, authentication, digital signature, and key management. Cryptographic tools help control access to information by making it unintelligible to unauthorized users and by protecting the integrity of transmitted or stored information.
Auditing and Monitoring	To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is necessary to determine what, when, and by whom specific actions have been taken on a system. Agencies do so by implementing software that provides an audit trail, or logs of system activity, that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities.
Physical Security	Physical security controls help protect computer facilities and resources from espionage, sabotage, damage, and theft. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, locks, and procedures for granting or denying individuals physical access to computing resources. Physical controls also include environmental controls such as smoke detectors, fire alarms, extinguishers, and uninterruptible power supplies. Considerations for perimeter security include controlling vehicular and pedestrian traffic. In addition, visitors' access to sensitive areas is to be managed appropriately.

Source: GAO-11-714.

For fiscal years 2013 and 2014, we, agencies, and inspectors general reported weaknesses in access controls for 22 of the 24 agencies. In fiscal year 2014, 12 agencies had weaknesses reported in protecting their networks and system boundaries, a reduction from the 17 agencies that had weaknesses in fiscal year 2013. For example, we found that 1 agency component's access control lists on a firewall had not prevented traffic coming or initiated from the public internet protocol addresses of a

contractor site and a U.S. telecom corporation from entering to its network. Additionally, for fiscal year 2014, 20 agencies had weaknesses reported in their ability to appropriately identify and authenticate system users, a slight increase from 19 of 24 in fiscal year 2013. To illustrate, in fiscal year 2014, 1 agency had not consistently applied proper password settings to mainframe service accounts, where those accounts were configured to never require password changes. Agencies also had weak password controls, such as using system passwords that had not been changed from the easily guessable default passwords.

In fiscal year 2014, 18 agencies had weaknesses reported in authorization controls, a reduction from the 20 agencies that had weaknesses in fiscal year 2013. One example of this weakness for fiscal year 2014 was that 1 agency had not consistently or in a timely manner removed, transferred, and/or terminated employee and contractor access privileges from multiple systems. Another agency had granted access privileges unnecessarily, which allowed users of an internal network to read and write files containing sensitive system information, including passwords, that were used to support automated data transfer operations between numerous systems. In fiscal year 2014, 4 agencies had weaknesses reported in encryption, down from 7 in fiscal year 2013.

In addition, 19 agencies had weaknesses reported in implementing an effective audit and monitoring capability. For instance, 1 agency had not effectively implemented audit and monitoring controls on a system where the servers and network devices were not sufficiently logging security-relevant events. Finally, 10 agencies had weaknesses reported in their ability to restrict physical access or harm to computer resources and protect them from unauthorized loss or impairment. For example, a contractor of an agency was granted physical access to a server room without the required approval of the office director. Without adequate access controls in place, agencies cannot ensure that their information resources are being protected from intentional or unintentional harm.

Agencies Did Not Fully
Implement Controls for
Configuration Management

Configuration management controls ensure that only authorized and fully tested software is placed in operation, software and hardware is updated, information systems are monitored, patches are applied to these systems to protect against known vulnerabilities, and emergency changes are documented and approved. These controls, which limit and monitor access to powerful programs and sensitive files associated with computer operations, are important in providing reasonable assurance that access controls and the operations of systems and networks are not compromised. To protect against known vulnerabilities, effective

procedures must be in place, current versions of vendor-supported software installed, and patches promptly implemented. Up-to-date patch installation helps mitigate known flaws in software code that could be exploited to cause significant damage and enable malicious individuals to read, modify, or delete sensitive information or disrupt operations.

In fiscal year 2014, 22 agencies had weaknesses reported in configuration management, a reduction from the 24 agencies that had weaknesses in fiscal year 2013. For fiscal year 2014, 17 agencies had weaknesses reported with installing software patches and implementing current versions of software in a timely manner, an improvement from the 23 reported in fiscal year 2013. One agency had not installed critical updates in a timely manner for several of its servers. Another agency was using an unsupported software application on its workstations, and a database system used to support the access authorization system was no longer supported. For fiscal year 2014, 14 agencies had weaknesses reported in authorizing, testing, approving, tracking, and controlling configuration changes. In fiscal year 2014, our work revealed that 1 agency had not effectively documented and approved configuration changes. Specifically, the agency did not request or approve 32 changes to mainframe production processing that had been recorded in the system logs.

Without a consistent approach to testing, updating, and patching software, agencies increase their risk of exposing sensitive data to unauthorized and possibly undetected access.

**More than Half of the Agencies
Did Not Segregate
Incompatible Duties**

Segregation of duties refers to the policies, procedures, and organizational structure that help to ensure that one individual cannot independently control all key aspects of a computer-related operation and thereby take unauthorized actions or gain unauthorized access to assets or records. Key steps to achieving proper segregation are ensuring that incompatible duties are separated and employees understand their responsibilities, and controlling personnel activities through formal operating procedures, supervision, and review.

In fiscal years 2013 and 2014, 15 agencies had weaknesses reported in implementing segregation of duties controls. For example, in fiscal year 2014, 1 agency had not implemented requirements for separating incompatible duties. Additionally, a developer from another agency had been authorized inappropriate access to the production environment of the agency's system. Further, another agency had not adequately implemented segregation of duties controls for IT and financial

	<p>management personnel with access to financial systems across several platforms and environments.</p> <p>Without adequate segregation of duties, agencies increase the risk that erroneous or fraudulent actions will occur, improper program changes will be implemented, and computer resources will be damaged or destroyed.</p>
Agencies Had Weaknesses in Continuity of Operations	<p>In the event of an act of nature, fire, accident, sabotage, or other disruption, an essential element in preparing for the loss of operational capabilities is having an up-to-date, detailed, and fully tested continuity of operations plan. This plan should cover all key functions, including assessing an agency's information technology and identifying resources, minimizing potential damage and interruption, developing and documenting the plan, and testing it and making necessary adjustments. If continuity of operations controls are faulty, even relatively minor interruptions can result in lost or incorrectly processed data, which can lead to financial losses, expensive recovery efforts, and inaccurate or incomplete mission-critical information.</p> <p>Eighteen agencies had weaknesses reported in continuity of operations practices for their agencies in fiscal years 2014 and 2013. Specifically, in 2014, 16 agencies did not have a comprehensive contingency plan. For example, 1 agency's contingency plans had not been updated to reflect changes in the system boundaries, roles and responsibilities, and lessons learned from testing contingency plans at alternate processing and storage sites. Additionally, 15 agencies had not regularly tested their contingency plans. For example, 1 agency had not annually tested contingency plans for 10 of its 16 systems.</p> <p>Until agencies address identified weaknesses in their continuity of operations plans and tests of these plans, they may not be able to recover their systems in a successful and timely manner when service disruptions occur.</p>
Agencies Did Not Effectively Manage Security	<p>An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented an agency-wide information security program to help them manage their security process. An agency-wide security program, as required by FISMA 2002, provides a framework for assessing and managing risk, including developing and implementing security policies and procedures, conducting security awareness training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Without a well-</p>

We and Inspectors General
Recommended Actions to
Strengthen Information
Security

designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources.

In fiscal year 2014, 23 agencies had weaknesses reported in security management, while 24 had them in fiscal year 2013. In one example, an agency had not fully developed and implemented components of its agency-wide information security risk management program that met FISMA's requirements. Specifically, the agency had established an enterprise risk management framework; however, security risks had not been fully communicated to data centers, regional offices, and medical facilities. In another example, the agency did not have effective procedures for testing and evaluating controls since the procedures did not prescribe effective tests of authentication controls.

Until agencies fully resolve identified deficiencies in their agency-wide information security programs, they will continue to face significant challenges in protecting their information and systems.

Over the last several years, we and agency inspectors general have made hundreds of recommendations to agencies aimed at improving their implementation of information security controls. These recommendations identify actions for agencies to take in protecting their information and systems. For example, we and inspectors general have made recommendations for agencies to correct weaknesses in controls intended to prevent, limit, and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on their systems. We have also made recommendations for agencies to implement their information security programs and protect the privacy of PII held on their systems.

However, many agencies continue to have weaknesses in implementing these controls in part because many of these recommendations remain unimplemented. Until federal agencies take actions to implement the recommendations made by us and the inspectors general, federal systems and information as well as sensitive personal information about the public will be at an increased risk of compromise from cyber-based attacks and other threats.

Federal Efforts Are Underway to Improve Security

Due to the increase in cyber security threats, the federal government has initiated or continued several efforts to protect federal information and information systems. The White House, OMB, and federal agencies have launched several government-wide efforts that are intended to enhance information security at federal agencies. These key efforts are discussed here.

Cybersecurity Cross-Agency Priority goals: Initiated in 2012, the cybersecurity Cross-Agency Priority (CAP) goals are an effort intended to focus federal agencies' cybersecurity activity on the most effective controls. For fiscal years 2013 and 2014, these goals included:

- **Trusted Internet Connections:** Trusted Internet Connections (TIC) aims to improve the federal government's security posture through the consolidation of external telecommunication connections by establishing a set of baseline security capabilities through enhanced monitoring and situational awareness of all external network connections. OMB established fiscal year 2014 targets of 95 percent for TIC consolidation and 100 percent for implementing TIC capabilities. OMB reported that agencies had achieved 95 and 92 percent implementation, respectively, for these TIC goals in fiscal year 2014.
- **Continuous monitoring:** Intended to provide near real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk management decisions based on increased situational awareness. OMB established a fiscal year 2014 target of 95 percent implementation for continuous monitoring and reported that the agencies had achieved 92 percent implementation.
- **Strong authentication:** Intended to increase the use of federal smartcard credentials, such as personal identity verification and common access cards that provide multifactor authentication and digital signature and encryption capabilities. Strong authentication can provide a higher level of assurance when authorizing users' access to federal information systems. OMB established a fiscal year 2014 target of 75 percent implementation for strong authentication. In its report on fiscal year 2014 FISMA implementation, OMB indicated that the 24 federal agencies covered by the CFO Act had achieved a combined 72 percent implementation of these requirements, but this

number dropped to only 41 percent implementation for the 23 civilian agencies when excluding DOD.²⁷

In fiscal year 2015, the administration added the anti-phishing and malware defense as a new goal for the CAP initiative.

The National Cybersecurity Protection System (NCPS): NCPS is a system of systems (also known as EINSTEIN) that is intended to deliver a range of capabilities including intrusion detection and prevention, analytics, and information sharing. The goal of EINSTEIN is to provide the federal government with an early warning system, improved situational awareness of intrusion threats, near real-time identification, and prevention of malicious cyber activity. This system was created in 2003 by US-CERT to help reduce and prevent computer network vulnerabilities across the federal government. The capabilities of NCPS are to include network "flow," intrusion detection, and intrusion prevention functions, as described in table 2.²⁸

²⁷Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act* (Washington D.C.: Feb. 27, 2015).

²⁸The Senate and House reports accompanying the *Consolidated Appropriations Act, 2014* included a provision for us to review NCPS. The objectives of our review are to determine the extent to which (1) NCPS meets stated objectives, (2) DHS has designed requirements for future stages of the system, and (3) federal agencies have adopted the system. Our final report is expected to be released later this year.

Table 2: National Cybersecurity Protection System Capabilities

Operational name	Capability provided	Description
EINSTEIN 1	Network flow	Provides an automated process for collecting, correlating, and analyzing agencies' computer network traffic information from sensors installed at their Internet connections. ^a
EINSTEIN 2	Intrusion detection	Monitors federal agency Internet connections for specific predefined signatures of known malicious activity and alerts the United States Computer Emergency Readiness Team (US-CERT) when specific network activity matching the predetermined signatures has been detected. ^b
EINSTEIN 3	Intrusion prevention	Automatically blocks malicious traffic from entering or leaving civilian executive branch agency networks. This capability is managed by Internet service providers, who administer intrusion prevention and threat-based decision making using DHS-developed indicators of malicious cyber activity to develop signatures. ^c

Source: GAO analysis of DHS documentation and prior GAO reports | GAO-15-714

^aThe network traffic information includes source and destination Internet Protocol addresses used in the communication, source and destination ports, the time the communication occurred, and the protocol used to communicate.

^bSignatures are recognizable, distinguishing patterns associated with a cyber attack, such as a binary string associated with a computer virus or a particular set of keystrokes used to gain unauthorized access to a system.

^cAn indicator is defined by DHS as human-readable cyber data used to identify some form of malicious cyber activity. These data are related to Internet Protocol addresses, domains, e-mail headers, files, and strings. Indicators can be either classified or unclassified.

The Continuous Diagnostics and Mitigation (CDM) Program: CDM is intended to provide federal departments and agencies with a basic set of tools to support the continuous monitoring of information systems. According to DHS, the program is intended to provide federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. These tools include sensors that perform automated searches for known cyber vulnerabilities, the results of which feed into a dashboard that alerts network managers. These alerts can be prioritized, enabling agencies to allocate resources based on risk. DHS, in partnership with the General Services Administration, has established a government-wide acquisition vehicle to allow federal agencies (as well as state, local, and tribal governmental agencies) to acquire CDM tools at discounted rates.

The National Initiative for Cybersecurity Education (NICE): NICE is an interagency effort coordinated by NIST to improve cybersecurity education, including efforts directed at training, public awareness, and the federal cybersecurity workforce. This initiative is intended to support the

federal government's evolving strategy for education, awareness, and workforce planning and provide a comprehensive cybersecurity education program. To meet NICE objectives, efforts were structured into the following four components:

1. **National cybersecurity awareness:** This component included public service campaigns to promote cybersecurity and responsible use of the Internet and to make cybersecurity popular for children. It was also aimed at making cybersecurity a popular educational and career pursuit for older students.
2. **Formal cybersecurity education:** Education programs encompassing K-12, higher education, and vocational programs related to cybersecurity were included in this component, which focused on the science, technology, engineering, and math disciplines to provide a pipeline of skilled workers for private sector and government.
3. **Federal cybersecurity workforce structure:** This component addressed personnel management functions, including the definition of cybersecurity jobs in the federal government and the skills and competencies they required. Also included were new strategies to ensure federal agencies can attract, recruit, and retain skilled employees to accomplish cybersecurity missions.
4. **Cybersecurity workforce training and professional development:** Cybersecurity training and professional development for federal government civilian, military, and contractor personnel were included in this component.

The Federal Risk and Authorization Management Program (FedRAMP): FedRAMP is a government-wide program intended to provide a standardized approach to security assessment, authorization,²⁹ and continuous monitoring for cloud computing products and services.³⁰

²⁹Security authorization is the official management decision given by a senior official of an organization to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the nation, based on the implementation of an agreed-on set of security controls.

³⁰FedRAMP's security assessment framework encompasses four process areas (document, assess, authorize, and monitor) that are based on the six steps within the framework described in NIST's *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

FedRAMP defines a set of controls for low and moderate impact-level systems according to the baseline controls in NIST SP 800-53 Revision 4³¹ and includes control enhancements related to the unique security requirements of cloud computing. All federal agencies must meet FedRAMP requirements when using cloud services and the cloud service providers must implement the FedRAMP security requirements in their cloud environment.

In addition, the cloud service providers must hire a FedRAMP-approved third-party assessment organization to perform an independent assessment to audit the cloud system and provide a security assessment package for review. The package will then be reviewed by the FedRAMP Joint Authorization Board,³² which may grant a provisional authorization. Federal agencies can leverage cloud service provider authorization packages for review when granting an agency authority to operate, where this reuse is intended to save time and money. After the cloud provider has received a FedRAMP authorization from the Joint Authorization Board or the agency, it must implement a continuous monitoring capability to ensure the cloud system maintains an acceptable risk posture.

The Cyber and National Security Team (E-Gov Cyber): OMB created the Cyber and National Security Team, called the E-Gov Cyber Unit, to strengthen federal cybersecurity through targeted oversight and policy issuance. The unit and its partners, the National Security Council, DHS, and NIST, are to oversee agency and government-wide cybersecurity programs, and oversee and coordinate the federal response to major cyber incidents and vulnerabilities. OMB reported that the unit found that more than half of incidents occurring at federal agencies could have been prevented by strong authentication. In addition, the unit intends to monitor implementation of critical DHS programs such as NCPS and CDM.

The 30-Day Cybersecurity Sprint: In June 2015, in response to the OPM security breaches and to improve federal cybersecurity and protect

³¹NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

³²The Joint Authorization Board is composed of the chief information officers from DOD, DHS, and the General Services Administration and establishes the baseline controls for FedRAMP and criteria for accrediting third-party independent assessment organizations.

systems against evolving threats, the Federal Chief Information Officer launched the 30-day Cybersecurity Sprint. As part of this effort, the Federal Chief Information Officer instructed federal agencies to immediately take a number of steps to further protect federal information and assets and to improve the resilience of federal networks. Specifically, federal agencies were to:

- Immediately deploy indicators provided by DHS regarding priority threat actor techniques, tactics, and procedures to scan systems and check logs. Agencies were to inform DHS immediately if indicators return evidence of malicious cyber activity.
- Patch critical vulnerabilities without delay. The vast majority of cyber intrusions exploit well-known vulnerabilities that are easy to identify and correct. Agencies were to take immediate action on the DHS vulnerability scan reports they receive each week and report to OMB and DHS on progress and challenges within 30 days.
- Tighten policies and practices for privileged users. To the greatest extent possible, agencies were to minimize the number of privileged users; limit functions that can be performed when using privileged accounts; limit the duration that privileged users can be logged in; limit the privileged functions that can be performed using remote access; and ensure that privileged user activities are logged and that such logs are reviewed regularly. Agencies were to report to OMB and DHS on progress and challenges within 30 days.
- Dramatically accelerate implementation of multi-factor authentication, especially for privileged users. Intruders can easily steal or guess usernames/passwords and use them to gain access to federal networks, systems, and data. Requiring the use of a personal identity verification card or alternative form of multi-factor authentication can significantly reduce the risk of adversaries penetrating federal networks and systems. Agencies were to report to OMB and DHS on progress and challenges in implementation of these enhanced security requirements within 30 days.
- In addition to providing guidance to the agencies, the Federal Chief Information Officer established the Cybersecurity Sprint Team to lead a review of the federal government's cybersecurity policies, procedures, and practices. According to OMB, the team is comprised of OMB's E-Gov Cyber and National Security Unit, the National Security Council Cybersecurity Directorate, DHS, and DOD. At the end of the review, the Federal Chief Information Officer is to create

and operationalize a set of action plans and strategies to further address critical cybersecurity priorities and recommend a federal civilian cybersecurity strategy. Key principles of the strategy are to include:

- **Protecting data:** Better protect data at rest and in transit.
- **Improving situational awareness:** Improve indication and warning.
- **Increasing cybersecurity proficiency:** Ensure a robust capacity to recruit and retain cybersecurity personnel.
- **Increasing awareness:** Improve overall risk awareness by all users.
- **Standardizing and automating processes:** Decrease time needed to manage configurations and patch vulnerabilities.
- **Controlling, containing, and recovering from incidents:** Contain malware proliferation, privilege escalation, and lateral movement. Quickly identify and resolve events and incidents.
- **Strengthening systems Life-cycle security:** Increase inherent security of platforms by buying more secure systems and retiring legacy systems in a timely manner.
- **Reducing attack surfaces:** Decrease complexity and number of things defenders need to protect.

Successful implementation of these government-wide efforts will be key steps to improving cybersecurity at federal agencies.

Agencies' Implementation of FISMA 2002 Requirements Was Mixed

The extent of agencies' implementation of FISMA 2002 requirements for establishing and maintaining an information security program from fiscal year 2013 to fiscal year 2014 varied.³³ For example, according to the reports by the inspectors general of the 24 CFO Act agencies, the number of agencies implementing risk management activities and documenting policies and procedures increased while the number of agencies planning for security, providing security training, and testing controls decreased. In addition, agency inspectors general, NIST, and OMB, with support from DHS, continued to address their responsibilities under FISMA 2002, but opportunities remain for improving FISMA reporting.

More Agencies Implemented Risk Management Activities

FISMA 2002 required that agencies periodically assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. These risk assessments help determine whether controls are in place to remediate or mitigate risk to the agency. NIST has issued several guides for managing risk.³⁴

According to NIST's *Guide for Applying the Risk Management Framework to Federal Information Systems*, risk management is addressed at the organization level, the mission and business process level, and the information system level. Risks are addressed from an organizational perspective with the development of, among other things, risk management policies, procedures, and strategy. The risk decisions made at the organizational level are to guide the entire risk management program. In addition, the activities for the risks that are addressed at the

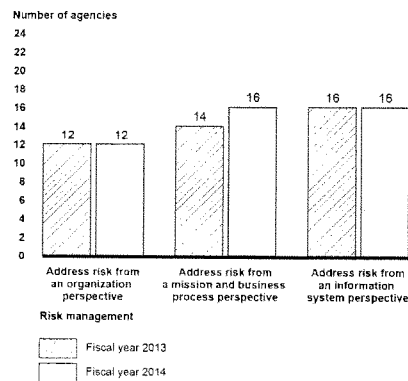
³³FISMA 2002 required that agencies implement security programs that included periodic assessments of risk; risk-based security policies and procedures; security training and awareness; periodic testing and evaluation of controls; a process for planning, implementing, evaluating, and documenting remedial actions; procedures for detecting, reporting, and responding to security incidents; and plans and procedures to ensure continuity of operations, among other items. These requirements of FISMA 2002 are continued in FISMA 2014 at 44 U.S.C. § 3554(b).

³⁴NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39 (Gaithersburg, Md.: March 2011); *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication 800-37 Revision 1; and *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1 (Gaithersburg, Md.: September 2012).

mission and business process levels include, among other things, defining and prioritizing the agency's mission and business processes and developing an organization-wide information protection strategy. There are various risk management activities for the risks that are addressed at the information system level, including categorizing organizational information systems, allocating security controls to organizational information systems, and managing the selection, implementation, assessment, authorization, and ongoing monitoring of security controls.

For fiscal years 2014 and 2013, inspectors general reported that 12 agencies had addressed risk from an organization perspective. In fiscal year 2014, inspectors general reported that 16 of 24 agencies had addressed risk from a mission or business perspective compared to 14 in fiscal year 2013. According to inspectors general, for fiscal years 2013 and 2014, 16 agencies had addressed risk from an information system perspective. Figure 4 shows examples of agencies' implementation of risk management program elements for fiscal years 2013 and 2014.

Figure 4: Examples of Agencies' Implementation of Risk Management Program Elements Reported for Fiscal Years 2013 and 2014



Source: GAO analysis of inspectors general *Federal Information Security Management Act* reports for fiscal years 2013 and 2014. | GAO-15-714

However, work by the inspectors general revealed weaknesses in risk management. According to OMB, inspectors general at seven agencies reported that their agency did not have a risk management program in place. The inspector general for one agency reported that, although the agency had implemented a risk governance structure, it had not fully identified or mitigated the enterprise-wide risks with appropriate risk mitigation strategies. Another inspector general reported that its agency did not have a current risk assessment for three of the seven systems in the sample. Managing risk is the center of an effective information security program; without effective risk management, agencies may not be fully aware of the risks to essential computing resources and may not be able to make informed decisions about needed security protections.

Most Agencies Had Documented Policies and Procedures

FISMA 2002 required agencies to develop, document, and implement policies and procedures that

- are based on risk assessments;
- cost-effectively reduce information security risks to an acceptable level;
- ensure that information security is addressed throughout the life cycle of each agency's information system; and
- ensure compliance with FISMA 2002 requirements, OMB policies and procedures, minimally acceptable system configuration requirements, and any other applicable requirements.

In fiscal years 2014 and 2013, most agency inspectors general reported that their agency had documented policies and procedures that were consistent with federal guidelines and requirements. Specifically, the number of agencies that documented policies and procedures increased in 8 of 11 categories, and remained the same in 3 categories since one inspector general did not report on these. Table 3 summarizes agencies' performance for fiscal years 2013 and 2014.

Table 3: Number of Agencies Documenting Information Security Policies and Procedures for Fiscal Years 2013 and 2014

FISMA reporting area		Policies and procedures in place during fiscal year 2013	Policies and procedures in place during fiscal year 2014
1	Risk management	18	20
2	Configuration management	22	23
3	Incident response and reporting	20	21
4	Security training	20	23
5	Remedial actions	21	23
6	Remote access management	16	18
7	Identify and access management	19	21
8	Continuous monitoring	17	21
9	Continuity of operations	22	21 ^a
10	Oversight of contractor systems	21	20 ^a
11	Security capital planning	21 ^a	21 ^a

Source: CyberScope submissions for fiscal years 2013 and 2014. | GAO-15-714

^aIn the CyberScope submission, one inspector general did not report on these programs and only 23 agencies were included.

In our prior work, we have also identified weakness in agencies policies and procedures for information security. In fiscal year 2014, we reported that six agencies we reviewed had not fully developed comprehensive policies and procedures for incident response. For example, only two of the six selected agencies had fully implemented policies that addressed roles, responsibilities, and levels of authority for incident response.³⁵ Similarly, we reported that several agencies had not established policies and procedures to oversee or assess the security of contractor systems.³⁶ Further, we found that one agency component's mainframe security policy did not address who can administer the security software configurations that control access to mainframe programs.³⁷ We recommended that these agencies develop and update policies and

³⁵GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (Washington, D.C.: Apr. 24, 2014).

³⁶GAO, *Information Security: Agencies Need to Improve Oversight of Contractor Controls*, GAO-14-612 (Washington, D.C.: Aug. 8, 2014).

³⁷GAO-15-337.

procedures for these areas. The agencies generally concurred with our recommendations.³⁸

Until all agencies properly document and implement policies and procedures, they may not be able to effectively reduce risks to their information and information systems, and the information security practices that are driven by these policies and procedures may be applied inconsistently.

**Number of Agencies with
Sufficient Security
Planning Decreased**

FISMA 2002 required agencies' information security programs to include plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. According to NIST, the purpose of a system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements.³⁹ The first step in the system security planning process is to categorize the system based on the impact to agency operations, assets, and personnel should the confidentiality, integrity, and availability of the agency's information and information systems be compromised. This categorization is then used to determine the appropriate security controls needed for each system. Another key step is selecting a baseline of security controls for each system and documenting those controls in the security plan.

In addition, NIST recommends that the plan be reviewed and updated at least annually. According to NIST, the security authorization package documents the results of the security control assessment and provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls. The package contains a security plan, security assessment report, and plan of action and milestones (POA&M). DHS's fiscal year 2014 reporting instructions request inspectors general to report on their agencies implementation of

³⁸GAO-14-354, GAO-14-612, and GAO-15-337.

³⁹NIST, *Guide for Developing Security Plans for Federal Information Systems*, Special Publication (SP) 800-18 Revision 1 (Gaithersburg, Md.: February 2006).

certain program attributes⁴⁰ such as whether (1) the agency has categorized information systems, (2) its security authorization package contained system security plan, security assessment report, POA&M, and accreditation boundaries, and (3) it has selected and implemented a tailored set of baseline security controls.

In fiscal year 2014, agency inspectors general at 18 agencies reported that their agency had categorized information systems in accordance with federal policies, a decrease from fiscal year 2013, in which 19 inspectors general reported that their agency had categorized their systems. In addition, fewer agencies selected an appropriately tailored set of baseline security controls. For instance, in fiscal year 2014, 15 inspectors general stated that their agency had appropriately selected a baseline of security controls, while 16 had reported for fiscal year 2013. In addition, in fiscal year 2014, 13 inspectors general reported that their agency had implemented a tailored set of baseline security controls, another decrease from fiscal year 2013, in which 14 agencies were reported for such controls.⁴¹

For fiscal year 2014, according to the inspectors general, 15 agencies had completed a security authorization package that contained a system security plan; 8 had not completed one; and 1 inspector general responded that the question was "not applicable." This is a decrease from fiscal year 2013, where 17 agencies had included such a security authorization package. In addition, inspectors general at 11 agencies reported that their agency had not always completed or properly updated their security plan. For example, a component of 1 agency had not completed one or more key elements of its system security plan, such as defining the system's accreditation boundary. Further, at another agency, five systems had been placed into production without a system security plan.

⁴⁰Attributes are additional questions in each of 11 areas as defined in DHS' FISMA reporting guidance to inspectors general. The attributes support the inspector's general assessment of his or her department's information security programs in those areas (see table 3 for a list of areas).

⁴¹In fiscal year 2014, the Inspector General for Commerce reported "not applicable" in this area. According to OMB, the Inspector General's FISMA audit scope was reduced as a result of (1) attrition of several key IT security staff, (2) the need to complete audit work assessing the security posture of key weather satellite systems that support a national critical mission, and (3) additional office priorities. The FISMA submission primarily focused on assessing policies and procedures, and covered a limited number of systems.

Until agencies appropriately develop and update their system security plans, officials will not be aware of system security requirements or whether controls are in place.

**Number of Agencies
Providing Sufficient
Security Awareness
Decreased and the
Percentage of Personnel
Receiving Specialized
Training Decreased**

FISMA 2002 required agencies to provide security awareness training to personnel, including contractors and other users of information systems that support the operations and assets of the agency. Training is intended to inform agency personnel of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks. FISMA 2002 also requires agencies to train and oversee personnel who have significant information security responsibilities. Providing training to agency personnel is critical to securing information and systems because people are one of the weakest links when securing systems and networks.

For fiscal year 2014, fewer agencies reported that at least 90 percent of their users had received security awareness training. The chief information officers for 22 agencies reported that they had provided annual security awareness training to at least 90 percent or more of their network users, which was a decrease from fiscal year 2013, when all 24 agencies reported that they had provided such training. Agency inspectors general reported similar results. For fiscal year 2014, inspectors general for 20 agencies reported that their agency had established a security awareness and training program, which was a decrease from fiscal year 2013, in which 21 agencies had established one. Similarly, they reported that fewer agencies had identified and tracked the status of security awareness training. Specifically, inspectors general for 16 agencies reported that their agency had identified and tracked the status of security awareness training in fiscal year 2014, a decrease from fiscal year 2013, in which 19 agencies had identified and tracked such training.

For fiscal year 2014, the percentage of personnel with significant security responsibilities who received training decreased from the previous year. In February 2015, OMB reported that, for fiscal year 2014, the 24 agencies provided training to an average of 80 percent of personnel who have significant security responsibilities, which reflects a decrease from the 92 percent reported for fiscal year 2013.

Without effective security awareness training, agency personnel may not have a basic understanding of information security requirements to protect the systems they use. In addition, personnel who did not take

specialized training may lack the knowledge, skills, and abilities consistent with their roles to protect the confidentiality, integrity, and availability of the information housed within the information systems to which they are assigned.

Fewer Agencies Are Periodically Testing and Continuously Monitoring Controls

FISMA 2002 required that federal agencies periodically test and evaluate the effectiveness of their information security policies, procedures, and practices as part of implementing an agency-wide security program. This testing is to be performed with a frequency depending on risk, but no less than annually. Testing should include management, operational, and technical controls for every system identified in the agency's required inventory of major systems. This type of oversight is a fundamental element that demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although control tests and evaluations may encourage compliance with security policies, the full benefits are not achieved unless the results are used to improve security.

For fiscal year 2014, inspectors general reported that fewer agencies had tested and evaluated security controls using appropriate assessment procedures to determine the extent to which the controls had been implemented correctly, operated as intended, and produced the desired outcome with respect to meeting the security requirements for the system. In fiscal year 2014, 16 inspectors general reported that their agency had assessed security controls, while 17 agencies had assessed such controls in fiscal year 2013.⁴²

As part of government-wide efforts to improve the testing of controls, agencies have begun steps to implement continuous monitoring of their systems. According to NIST, the goal of continuous monitoring is to transform the otherwise static test and evaluation process into a dynamic risk mitigation program that provides essential, near real-time security status and remediation. NIST defines information system continuous monitoring as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management

⁴²The Commerce Inspector General reported "not applicable" in this area in fiscal year 2014.

decisions.⁴³ Since March 2012, continuous monitoring has also been designated as a cross-agency priority area for improving federal cybersecurity.

Although OMB reported overall increases in the 24 agencies' continuous monitoring (from 81 percent in fiscal year 2013 to 92 percent in fiscal year 2014) of controls, inspectors general reported that fewer agencies had continuously monitored controls for their systems. For example, for fiscal year 2014, 12 inspectors general stated that their agency had ensured information security controls were being monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting a security impact analysis of the associated changes, and reporting the security state of the system to designated organizational officials. This is a decrease from fiscal year 2013, when 14 agencies had monitored security controls on an ongoing basis.⁴⁴

If controls are not effectively tested or properly monitored, agencies will have less assurance that they have been implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements of the agency.

Increasing Number of Agencies are Generally Implementing Elements of a Remediation Program, but Weaknesses Remain

FISMA 2002 required agencies to plan, implement, evaluate, and document remedial actions to address any deficiencies in their information security policies, procedures, and practices. In addition, NIST guidance states that federal agencies should develop a POA&M for information systems to document the agency's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.⁴⁵ Furthermore, the POA&M should identify, among other things, the resources required to accomplish the tasks, and scheduled

⁴³NIST, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST Special Publication 800-137 (Gaithersburg, Md.: September 2011).

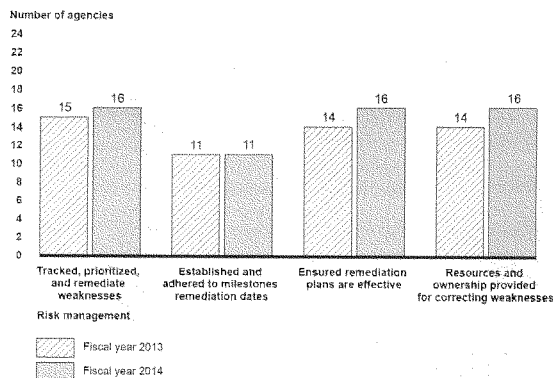
⁴⁴In fiscal year 2014, the Commerce Inspector General reported "not applicable" in this area.

⁴⁵NIST, *Special Publication (SP) 800-53A, Revision 4* (Gaithersburg, Md.: December 2014).

completion dates for the milestones. According to OMB, remediation plans assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

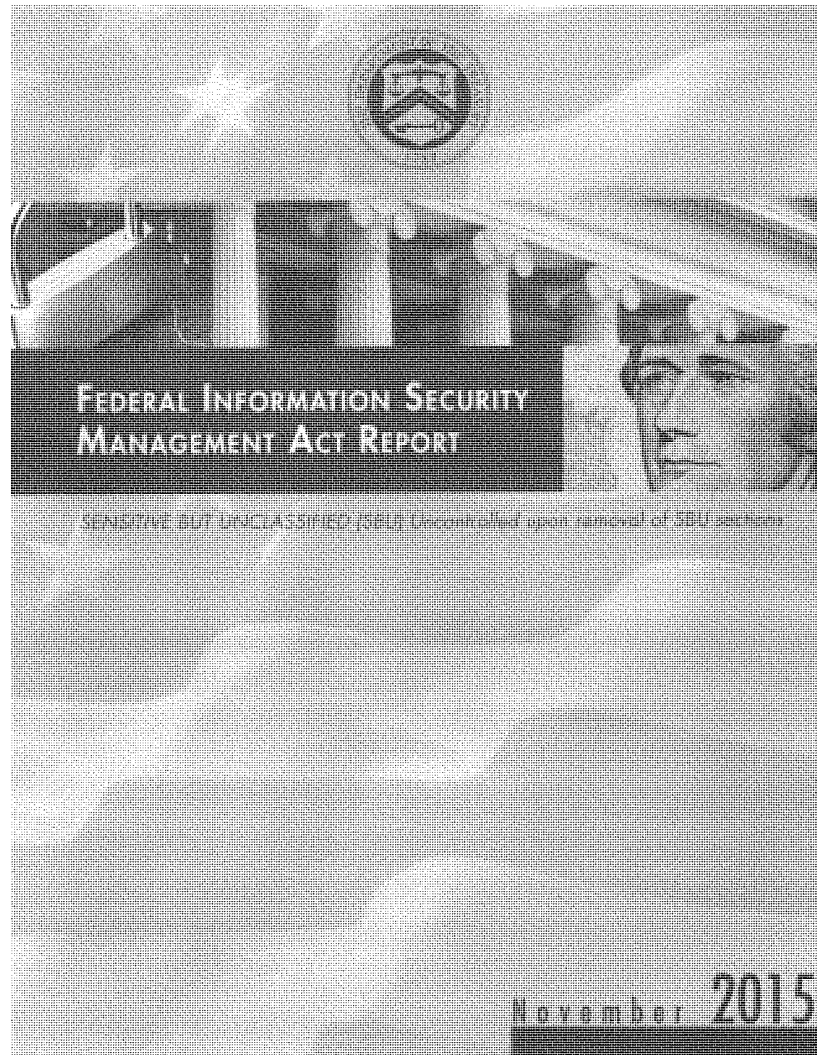
For fiscal year 2014, the number of agencies implementing certain elements of their remediation programs increased or remained the same. For fiscal year 2014, inspectors general reported that 16 agencies had tracked, prioritized, and remediated weaknesses, compared to 15 for fiscal year 2013. In addition, 11 agencies had established and adhered to milestone remediation dates in both fiscal years. Further, 16 agencies were reported having an effective remedial action plan in fiscal year 2014, an increase from fiscal year 2013, in which 14 reported having such a plan. For fiscal year 2014, 16 inspectors general reported that their agency had ensured resources and ownership were provided for correcting weaknesses, which is also an increase from 14 in fiscal year 2013. Figure 5 shows agencies' remediation program efforts for fiscal years 2013 to 2014.

Figure 5: Agencies' Implementation of Remediation Program Elements Reported for Fiscal Years 2013 and 2014



Source: GAO analysis of inspectors general Federal Information Security Management Act reports for fiscal years 2013 and 2014. | GAO-15-714

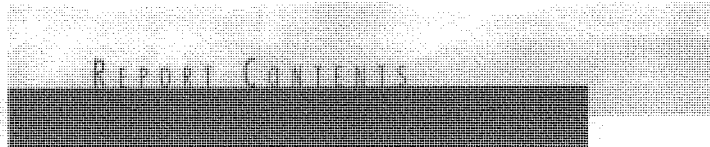
REPORT SUBMITTED BY SUBCOMMITTEE CHAIRWOMAN
BARBARA COMSTOCK





SENSITIVE BUT UNCLASSIFIED (SBU) Uncontrolled upon removal of SBU sections

November 2015



Section 1 – Treasury Signed Letter

Section 2 – 2015 Annual FISMA Report

Chief Information Officer Section Report

Inspector General Section Report

Senior Agency Official for Privacy Section Report

Section 3 – OIG/TIGTA Narrative Audit Reports

OIG & TIGTA for Sensitive But Unclassified Systems

OIG for National Security Systems

Section 4 – Privacy Artifacts

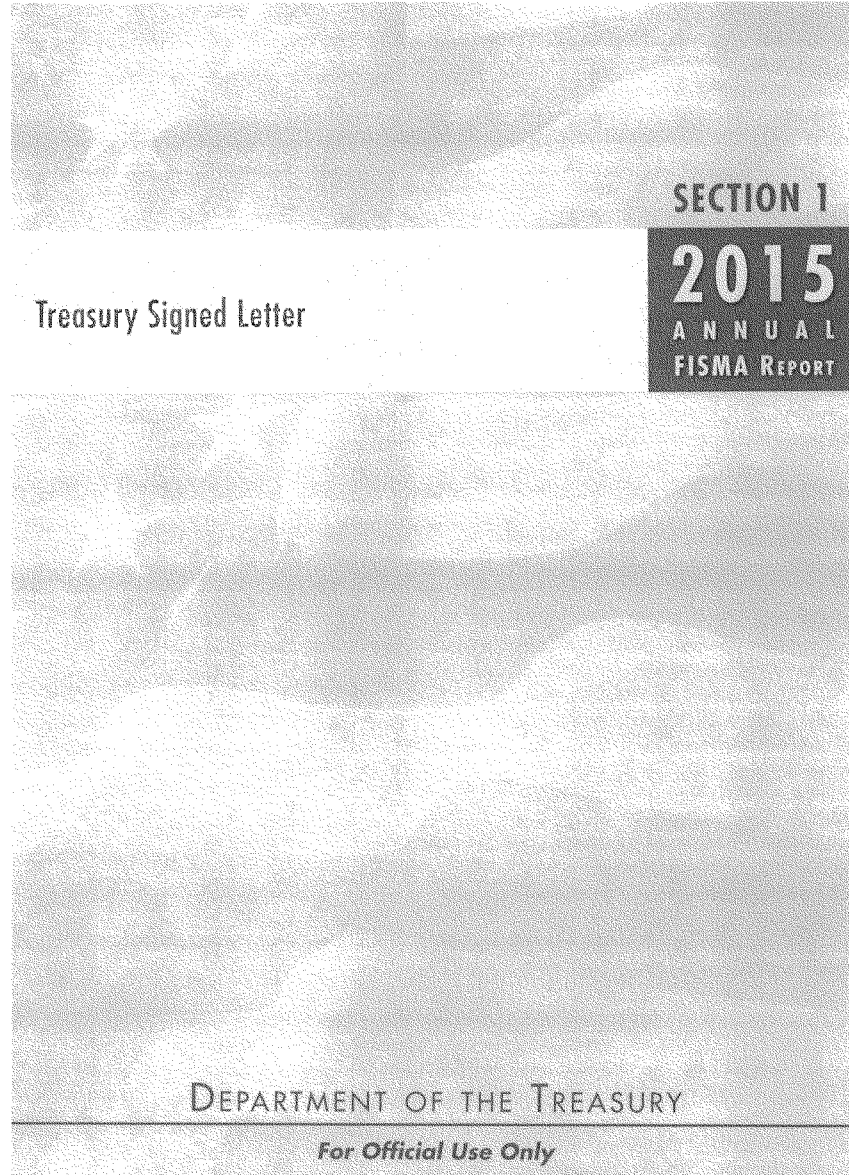
Implementation Plan and Progress Update to Eliminate Unnecessary Use of SSNs

Implementation Plan and Progress Update on Review and Reduction of Holdings of PII

Breach Notification Policy (TD 25-08)

Description of Privacy Training for Agency Employees and Contractors

Description of the Agency's Privacy Program





DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

SECRETARY OF THE TREASURY

November 23, 2015

The Honorable Shaun Donovan
Director
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Director Donovan:

I am pleased to submit the Department of the Treasury's Annual Federal Information Security Management Act (FISMA) Report for 2015. In accordance with guidance from the Office of Management and Budget (OMB) and Department of Homeland Security (DHS), our submission (via the CyberScope reporting tool) includes the following:

- This official letter and executive summary providing my assessment of the adequacy and effectiveness of the Department's information security and privacy policies, procedures, and practices;
- The Chief Information Officer's Annual Information Technology Security Report;
- The independent performance evaluations from the Treasury Office of the Inspector General (OIG) and the Treasury Inspector General for Tax Administration (TIGTA);
- The Senior Agency Official for Privacy's (SAOP) Report

Should you have any questions regarding this report, please contact Sanjeev "Sonny" Bhagowalia, Deputy Assistant Secretary for Information Systems and Chief Information Officer, at 202-927-0777.

Sincerely,

A handwritten signature in black ink, appearing to read "Jacob J. Lew".

Jacob J. Lew

Enclosures

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary: FY 2015 Annual FISMA Report

United States Code Title 44, Chapter 35, Subchapter II requires Federal departments and agencies to annually prepare a report on the adequacy and effectiveness of information security policies, procedures, and practices. By law, the report is submitted to the Office of Management and Budget, the Department of Homeland Security, the Comptroller General, and several Congressional committees.

Within Treasury, the Office of the Chief Information Officer (CIO) compiles this report, which consists of a report from the CIO, a report and artifacts from the Senior Agency Official for Privacy, and summary and narrative reports from the Office of the Inspector General (OIG) and the Treasury Inspector General for Tax Administration (TIGTA).

FY 2015 Accomplishments and Next Steps

In FY 2015, we attained a number of milestones, including:

- Exceeded the CAP Secure Authentication goals during the Cyber Sprint by accelerating implementation of required use of Personal Identity Verification (PIV) cards for logical authentication to network accounts.
- Concluded another Cyber Sprint initiative by completing initial security reviews of 236 systems preliminarily identified as High Value Assets.
- Achieved an initial operating capability for Data Loss Prevention at two of five Trusted Internet Connections to inspect outbound email generated by non-IRS bureaus for sensitive information.
- Developed and formalized a Department-wide Framework for Information Security Continuous Monitoring (ISCM) that establishes a consistent risk-based process and set of practices for bureau transition from static, three-year system accreditation cycles to ongoing authorization.

Treasury remains committed to providing appropriate protection of our critical information and systems. The results of Treasury's 2015 independent FISMA evaluation indicate that Treasury continues to strengthen its information security and privacy programs. However, some areas remain in need of improvement. We will use the recommendations issued by our Inspectors General to help guide further improvements in the coming year. In addition, the Department is preparing to initiate Phase 1 of the DHS Continuous Diagnostics and Mitigation (CDM) program. Throughout FY 2016, new IT management capabilities are expected to be introduced that will increase the automation of asset management and ultimately provide near-real-time awareness of an enterprise-wide cybersecurity posture.

Chief Information Officer (CIO) Section

The CIO report section demonstrates that Treasury is meeting many cybersecurity targets, but also shows areas needing improvement. The CIO was asked to report status on 80 metrics, including those related to the Administration's Cross-Agency Priority (CAP) areas for Cybersecurity, Key FISMA Metrics, and Initial Baseline Metrics. These include:

CAP Performance Areas for Cybersecurity

Throughout the past year, Treasury made consistent improvements toward meeting Administration targets for the three Cybersecurity CAP goals.

1. Information System Continuous Monitoring (ISCM): routine automated scanning of networked assets, configurations, and vulnerabilities to ensure adequate security controls.

As of the end of FY 2015, Treasury has exceeded the Administration's FY 2017 target of 95 percent asset coverage for four of the six ISCM metrics: (i) management of authorized hardware devices (100 percent), (ii) management of authorized software (96 percent), (iii) vulnerability management (98 percent), and (iv) secure configuration management (99 percent). The Department remained below the Administration's 95 percent targets for detection of unauthorized hardware and protection from unauthorized software due to gaps in deployment of tools to provide these capabilities. Treasury expects that implementation of Phase 1 of the Continuous Diagnostics and Mitigation (CDM) program will address these gaps. Full implementation of these tools is planned by Q4 FY2016.

2. Strong Authentication: issuing and *requiring the use of* Personal Identity Verification (PIV) credentials for logical access to Treasury networks.

The Department has met or exceeded the Administration's FY 2017 targets for requiring the use of PIV cards for logical access to Treasury network accounts. During the Cyber Sprint, Treasury implemented PIV-required authentication for 100 percent of privileged users, meeting the adjusted CAP target. In addition, by the end of FY 2015, the Department had converted 96 percent of unprivileged users to PIV-required authentication, exceeding the Administration's target of 85 percent.

3. Anti-Phishing and Malware Defense (APMD): implementation of security measures to reduce exposure to common network threat vectors.

In FY 2015, Treasury exceeded the 90 percent CAP target for four out of four "Blended Defense" metrics, three out of five Malware Defense metrics, and four out of seven Anti-Phishing Defense metrics. This met the CAP threshold for Blended Defense and Malware Defense. In the coming year, the Department will implement activities to bolster its Anti-Phishing defenses, including the launch of an enterprise-wide program to increase the number of users tested with phishing exercises.

Key FISMA Metric Performance Areas

The *FY15 Chief Information Officer Annual Federal Information Security Management Act Metrics* included a significant number of items designated as "Key FISMA Metrics." This summary focuses on Treasury's progress in those performance areas. Additional FISMA Metrics are addressed in the preceding summary of progress toward meeting the CAP goals for Cybersecurity.

1. User Training and Education – Treasury determined that, as of June 30, 2015, 98 percent of its users successfully completed annual security awareness training, while 99 percent of its users with significant security responsibilities received specialized security training in FY 2015.

2. System Authorization – As of June 30, 2015, 90 percent of Treasury systems had a current, signed authorization to operate.
3. Remote Access Connection – Treasury bureaus reported that 100 percent of the connections that users employ to remotely access Treasury IT environments utilize NIST-approved cryptography, a time-out after 30 minutes of inactivity, and preventions of users from connecting to Treasury’s trusted networks with untrusted external networks. In addition, 99 percent of these accesses are scanned for malware upon connection—an improvement from 92 percent in FY 2014.
4. Mobile Device Encryption – Treasury bureaus reported that at least 99.5 percent of their laptops, netbooks, tablet computers, and smartphones encrypt data at rest. This represents an improvement from FY 2014, when only 98 percent of smartphones and less than 95 percent of tablets encrypted stored data.
5. Network Access Control – In the FY 2015 FISMA Metrics, OMB and the Department of Homeland Security (DHS) introduced a number of new security objectives. Treasury is in the early stages of addressing many of these. Among the most important is the deployment of Network Access Control technology, which serves to block unauthorized devices from accessing enterprise networks. For FY 2015, Treasury determined that 64 percent of its network fabric was protected by this technology. The Department expects that the implementation of CDM Phase 1 in FY 2016 will help increase the use of this technology across all bureaus.

Senior Agency Official for Privacy (SAOP) Section

OMB requires departments and agencies to include in their annual FISMA submissions a report from the SAOP responding to several questions regarding handling of privacy issues, along with a handful of artifacts demonstrating progress in meeting privacy mandates. The Office of Privacy, Transparency, and Records prepares this section of the report. Treasury’s report addresses such issues as our personally identifiable information (PII) holdings, privacy impact assessments, and system of record notices. We also submit required privacy artifacts, including a summary of progress on reducing PII holdings and eliminating unnecessary use of Social Security Numbers (SSN). The artifacts indicate that bureaus are continuing their efforts to achieve those goals. During FY 2015, SSNs were masked (exposing only the last four digits) on 17.5 million taxpayer notice forms and were completely eliminated from 5.2 million notices.

The privacy artifacts are not transmitted to Congress.

Inspectors General (IG) Section

Under FISMA, OIG and TIGTA, referred to collectively as the “IGs,” annually review agency security practices in 10 areas. These practices reduce risks to agency information systems. The auditors picked a sample set (15 non-Internal Revenue Service (IRS) systems and 10 IRS systems) out of the Department’s inventory of 364 non-national security systems for this year’s review. The OIG also conducted a separate evaluation of the Department’s National Security Systems (NSS), including a review of two collateral NSS. The IG section contains the results of these evaluations.

The IG section contains responses to 92 yes/no questions. The IGs indicate “no” to these questions when they identify a weakness at any one bureau during their annual FISMA

evaluations. For FY 2015, the IGs recorded “No” responses to 34 questions. The TIGTA’s negative responses, which particularly cited weaknesses in configuration and access management, were based exclusively on evaluation of the Internal Revenue Service (IRS). For non-IRS bureaus, many of the identified issues relate to lapses in documentation, as documented in the IG’s narrative report.

The Office of the CIO will closely monitor bureau remediation of the FISMA compliance issues identified in the IG section of the annual FISMA submission. Treasury has in place existing oversight mechanisms to track bureau mitigation activities. For our non-IRS bureaus, mitigation plans are included in the management response to the Inspector General’s FY 2015 FISMA Audit report (see below). At the IRS, remediation of many compliance issues will depend upon the introduction of new continuous monitoring capabilities expected to be introduced in FY 2016 under the DHS CDM program. Treasury is leading the CDM engagement with DHS and will work with IRS management to ensure that the CDM tools are appropriately deployed across the IRS enterprise.

IG Narrative Evaluation Reports

On November 12, 2015, the OIG provided its final FISMA evaluation reports for both the collateral NSS and the unclassified systems. TIGTA’s final report has been consolidated with the OIG’s report. Last year, the combined IG reports identified 30 recommendations for unclassified and collateral national security systems. This year, the OIG made 24 recommendations. Treasury anticipates agreement with all of the OIG’s findings and recommendations. The Office of the CIO will work with Treasury bureaus to ensure the findings are addressed in the time frames specified in the bureau corrective action plans summarized in the Department’s management response, taking a risk-based approach to other vulnerabilities. The OIG’s narrative reports present more details on the findings and recommendations. TIGTA does not issue recommendations as part of its annual FISMA evaluation.

Incidents reported to the United States Computer Emergency Readiness Team (US-CERT)

The Federal Information Security Modernization Act of 2014 (FISMA 2014) requires agencies to provide a total count of information security incidents occurring during the prior year, along with a description of each “major” incident and additional details for each “major” incident that involved a breach of PII. To facilitate this reporting, FISMA 2014 required the Office of Management and Budget to develop guidance on what constitutes a “major” incident to guide agencies in meeting the FISMA incident reporting requirements applicable thereto. Because draft guidance on determination of “major” incidents was not provided to agencies until September 2015, Treasury was not able to establish mechanisms to capture all of the incident information required to determine whether security incidents should be designated as “major” and thereby ensure the application of appropriate and timely reporting procedures. Based on data captured by the incident reporting mechanisms that Treasury had in place throughout FY 2015, one incident involving breach of PII was identified that likely would have been categorized as “major” had appropriate guidance been available at the time of occurrence.

In May 2015, the Internal Revenue Service (IRS) identified a breach of taxpayer information that was executed using the Get Transcript web application. Unknown threat actors leveraged the system beginning in February 2015, using personally identifiable information taken from non-Treasury sources to inappropriately obtain information on taxpayer accounts. The perpetrators

impersonated individual taxpayers by using their specific personal information to clear a multi-step authentication process similar to that used by financial institutions and credit reporting agencies to identify individuals. A review of more than 23 million uses of the Get Transcript application identified approximately 330,000 instances in which perpetrators successfully impersonated individual taxpayers, and another 281,000 attempts in which impersonation failed. The incident potentially resulted in the breach of data contained within IRS transcripts, which can contain all information included on an individual tax return. This includes names, addresses, and social security numbers of taxpayers and their dependents.

Following detection of the inappropriate access activities, the Get Transcript application was taken offline. The IRS Computer Security Incident Response Center reported the incident to the Department's Government Security Operations Center, which in turn reported the incident to US-CERT. The IRS offered free credit monitoring to all taxpayers potentially impacted by the incident, both those who were successfully impersonated and those for whom impersonation failed. At their option, taxpayers will also be provided with personal identification numbers (PINs) that they can use to authenticate their tax returns beginning with the 2016 filing season.

The IRS continues to work to strengthen the security of the Get Transcript application. The incident remains under investigation by the IRS Criminal Investigation division and the TIGTA.

Total Number of Cyber Incidents in FY 2015

The summary matrix below tracks the number of cyber incidents that Treasury reported to US-CERT through the US-CERT Incident Notification System in FY 2015. The matrix breaks out the cyber incidents by incident type (reflected in the US-CERT categorization) and by location within the Department (i.e., affected bureau).

	CAT 1	CAT 2	CAT 3	CAT 4	CAT 5	CAT 6	CAT 0	Uncategorized	Total By Location
BEP	2	0	0	0	0	3	0	0	5
FS	16	0	1	14	0	13	1	0	45
DO	7	1	2	3	0	2	0	1	16
FinCEN	5	0	0	0	0	3	0	0	8
IRS	201	2	47	406	0	1	0	4	661
Mint	4	0	1	0	1	0	0	0	6
OCC	8	0	3	1	0	1	0	1	14
OIG	0	0	0	1	0	0	0	0	1
TIGTA	7	0	0	1	0	5	0	1	14
TTB	0	0	3	1	0	1	0	0	5
Total By Type	250	3	57	427	1	29	1	7	775

Table 1 – Cyber Incidents by Incident Type and Agency Location

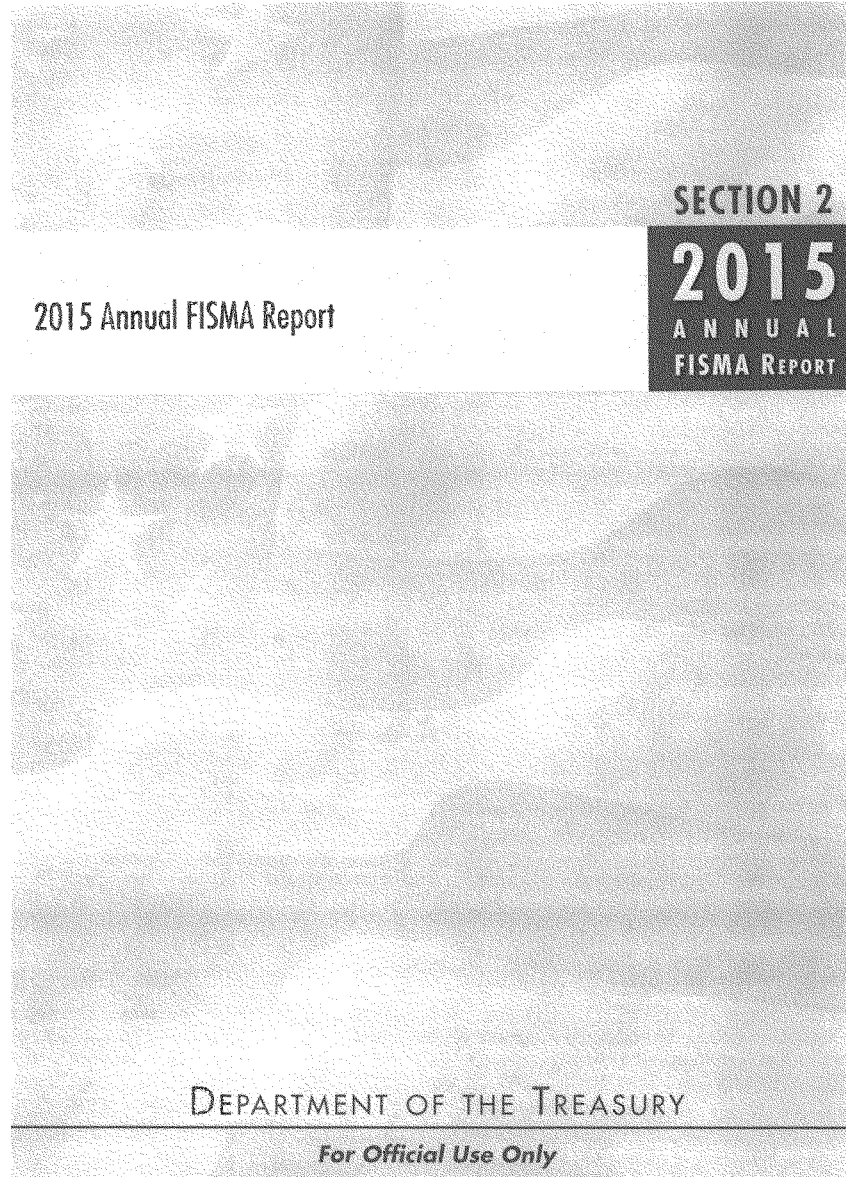
For additional context, the table below tracks the number of incidents that Treasury reported to US-CERT through the US-CERT Incident Notification System in each of the last four fiscal years, and breaks out the percentage of these that involved the loss of paper records.

Fiscal Year	Total Incidents Reported to US-CERT	Percent of reports to US-CERT involving lost paper records
FY 15	2,176	31%
FY 14	3,555	41%
FY 13	3,014	54%
FY 12	3,851	55%

Table 2 – Trending of Reported Paper Record Losses over Time

Over the past four fiscal years, the percentage of reported incidents of lost paper records as a function of all reported incidents has declined steadily. This trend is the result of reduced reliance on paper records across the Department, ongoing efforts to reduce the prevalence of social security numbers in paper communications, increasing employee awareness of personally identifiable information and related protection requirements, and, in FY 2015, gradual adoption of new US-CERT guidance on reporting of lost paper records. Going forward, the Department does not anticipate reporting additional lost paper records to US-CERT due to changes in US-CERT reporting guidance.

Additional changes to US-CERT reporting guidance issued at the beginning of FY 2015 were not adopted by the Department until the end of the fiscal year due to required extensive changes to incident reporting ticketing systems. Further changes will be needed in FY 2016 to enable correlation of reported incidents to Treasury's FISMA system inventory and related information concerning the impact levels of systems affected by cyber incidents.



Chief Information Officer
Section Report

2015
ANNUAL
FISMA Report

DEPARTMENT OF THE TREASURY

For Official Use Only

Chief Information Officer

Section Report

2015
Annual FISMA
Report

Department of the Treasury

Section 1A: System Inventory

1.1 For each FIPS 199 impact level, what is the total number of operational unclassified information systems by organization (i.e. Bureau or Sub-Department Operating Element) categorized at that level? (Organizations with fewer than 5,000 users may report as one unit.) Answer in the table below.

		1.1.1 Organization-Operated Systems	1.1.2 Contractor-Operated Systems	1.1.3 Systems (from 1.1.1 and 1.1.2) with Security ATO (signed, in scope)
BEP	High	0	0	0
	Moderate	25	3	14
	Low	8	0	0
	Not Categorized	0	0	0
	Sub-Total	33	3	14
CDFI	High	0	0	0
	Moderate	3	0	3
	Low	0	0	0
	Not Categorized	0	0	0
	Sub-Total	3	0	3
DO	High	10	3	13
	Moderate	21	9	30
	Low	6	1	9
	Not Categorized	0	0	0
	Sub-Total	39	13	52
FINCEN	High	9	0	9
	Moderate	2	0	2
	Low	1	0	1
	Not Categorized	0	0	0
	Sub-Total	12	0	12
IRS	High	6	0	5
	Moderate	137	2	126
	Low	0	0	0
	Not Categorized	0	0	0
	Sub-Total	143	2	131
MINT	High	0	0	0
	Moderate	14	2	16
	Low	1	0	1
	Not Categorized	0	0	0
	Sub-Total	15	2	17

Section 1A: System Inventory				
		1.1.1 Organization-Operated Systems	1.1.2 Contractor-Operated Systems	1.1.3 Systems (from 1.1.1 and 1.1.2) with Security ATO (signed, in scope)
OCC	High	0	0	0
	Moderate	10	2	12
	Low	0	0	0
	Not Categorized	0	0	0
	Sub-Total	10	2	12
OIG	High	0	0	0
	Moderate	1	0	1
	Low	0	0	0
	Not Categorized	0	0	0
	Sub-Total	1	0	1
TIGTA	High	0	0	0
	Moderate	2	0	2
	Low	0	0	0
	Not Categorized	0	0	0
	Sub-Total	2	0	2
TTB	High	0	0	0
	Moderate	21	0	21
	Low	1	0	1
	Not Categorized	0	0	0
	Sub-Total	22	0	22
BFS	High	16	1	17
	Moderate	39	3	41
	Low	5	0	5
	Not Categorized	0	0	0
	Sub-Total	60	4	63
Agency Totals	High	41	4	44
	Moderate	275	21	268
	Low	24	1	17
	Not Categorized	0	0	0
	Total	340	26	329

Section 1B: System Inventory

1.2 How many endpoints belong to systems without a valid ATO?

Section 1B: System Inventory

1049

- 1.3 How many public facing systems are without a valid ATO?

1

Section 2A: ISCM - Hardware/Software Asset Management

Hardware Asset Management

- 2.1 What is the total number of the organization's hardware assets connected to the organization's unclassified network(s)?

176008

- 2.1.1 Percent (%) of assets from 2.1 that store (e.g., on an endpoint or maintained as a record in an external asset management database) meta-data (e.g. system association, owner, location)?

89%

- 2.1.2 What is the total number of endpoints connected to the organization's unclassified network(s)?

129098

- 2.2 Percent (%) of the organization's network fabric covered by a capability to detect and alert on the addition of unauthorized hardware assets onto the organization's network.

83%

Comments:

Status as of 9/25/2015. The Department has not yet achieved the 95% CAP target for this metric because not all bureaus currently have this capability. Implementation of CDM Phase 1 in FY 2016 is expected to help address the gap.

- 2.3 Percent (%) of the organization's network fabric covered by an automatic capability (scans/device discovery processes) that provides enterprise-level visibility into the current state of all hardware assets.

100%

Comments:

Status as of 9/25/2015

- 2.4 What is the mean time to detect a new device (time between scans in 2.2)?

1.0

Comments:

days

- 2.5 Percent (%) of the organization's registered network fabric covered by a Network Access Control switching technology that blocks unauthorized devices.

64%

Software Asset Management

Section 2A: ISCM - Hardware/Software Asset Management

2.6 Percent (%) of endpoints from 2.1.2 covered by an automated software asset inventory capability to scan the current state of installed software (e.g., .bat, .exe, .dll).

96%

Comments: Status as of 9/25/2015

2.7 Percent (%) of endpoints from 2.1.2 covered by a desired-state software asset management capability to detect and block unauthorized software from executing (e.g., AppLocker, certificate, path, hash value, services, and behavior based whitelisting solutions).

91%

Comments: Status as of 9/25/2015: The Department has not yet achieved the 95% CAP target for this metric because not all bureaus currently have this capability. Implementation of CDM Phase 1 in FY 2016 is expected to help address the gap.

2.8 How many major application databases does the organization maintain?

276

2.9 Percent (%) of the organization's network fabric that undergoes periodic discovery scanning specifically for the purpose of identifying and enumerating databases.

18%

Section 2B: ISCM - Secure Configuration Management

2.10 Please complete the table below. Future configurations will be added as needed. Data calls for layer 2, layer 3, mobile, printers, or other devices or operating systems will be used as needed.

Comments: Status as of 9/25/2015

218

Section 2B: ISCM - Secure Configuration Management						
List of top U.S. Government Operating Systems, as reported in SCAP feeds	2.10.1 What is the number of hardware assets with each OS?	2.10.2 What is the common security configuration baseline for each OS listed? (e.g., USGCB)	2.10.3 How many configuration exceptions are granted by the enterprise?	2.10.4 What is organization's enterprise policy for maximum audit interval (target)?	2.10.5 What is organization's enterprise average audit interval (actual)?	2.10.6 Percent (%) of assets in 2.10.1 covered by the auditing activities described in 2.10.4 and 2.10.5
Windows 8.x	149	United States Government Computer Baseline (USGCB)	0	14.00	1.00	100%
Windows 7.x	113,374	United States Government Computer Baseline (USGCB)	0	14.00	24.53	100%
Windows Vista	0	N/A	N/A	N/A	N/A	N/A
Windows Unsupported (include XP)	371					
Windows Server 2003	2,491	Center for Internet Security (CIS)	0	14.00	24.86	95%
Windows Server 2008	6,574	Defense Information Systems Agency (DISA STIG)	0	14.00	17.65	99%
Windows Server 2012	905	United States Government Computer Baseline (USGCB)	0	14.00	11.12	1%
Linux (all versions)	2,570	Center for Internet Security (CIS)	0	14.00	18.59	96%
Unix / Solaris (all versions)	1,627	Center for Internet Security (CIS)	0	14.00	18.88	100%
Mac OS X	362	Defense Information Systems Agency (DISA STIG)	0	14.00	23.96	100%
Section 2C: ISCM - Vulnerability and Weakness Management						

2.11 Percent (%) of hardware assets listed in 2.1 assessed using credentialed scans with Security Content Automation Protocol (SCAP) validated vulnerability tools:

98%

Comments: Status as of 9/25/2015

Section 2C: ISCM - Vulnerability and Weakness Management

2.12 What is the mean time between vulnerability scans?

9.9

Comments: days

2.13 Percent (%) of the databases in 2.8 that undergo periodic vulnerability scanning with a special purpose database vulnerability scanner.

57%

2.14 What is the mean time to mitigate for high findings?

26.2

Section 3: Identity Credential and Access Management

Unprivileged Network Users

3.1 How many users have unprivileged network accounts? (Exclude privileged network accounts and non-user accounts.)

91223

Comments: Status as of 10/15/2015

3.1.1 Percent (%) of users from 3.1 technically required to log onto the network with a two-factor PIV card or NIST Level of Assurance (LOA) 4 credential.

98%

Comments: Status as of 10/15/2015

Privileged Network Users

3.2 How many users have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.)

4475

3.2.1 Percent (%) of users from 3.2 technically required to log onto the network with a two-factor PIV card or NIST Level of Assurance (LOA) 4 credential.

100%

Comments: Status as of 10/15/2015

3.3 Percent (%) of privileged network users that had their privileges reviewed this year.

97%

3.4 Percent (%) of privileged network users that had their privileges adjusted or terminated after being reviewed this year.

21%

Section 3: Identity Credential and Access Management

Internal Systems

- 3.5 Percent (%) of the organization's internal systems configured to require PIV authentication.
68%
- 3.6 Percent (%) of the organization's government service portals (e.g., Max.gov Portal, MyEPP) that enforce PIV authentication for cross-agency federal customers. (If none are provided, answer N/A.)
2%

Remote and Mobile Device Access Solutions

- 3.7 How many users log onto the organization's remote access solution(s) to obtain access to the organization's desktop LAN/WAN resources or services?
57171
- 3.7.1 Percent (%) of the users reported in 3.7 required to use two-factor PIV card authentication to remotely log onto the organization's desktop LAN/WAN resources or services
78%
- Comments: Status as of 10/15/2015
- 3.8 How many users are enabled to remotely log onto the organization's LAN/WAN resources or services from mobile devices?
12515
- 3.8.1 Of the organization's users who remotely access desktop LAN/WAN resources or services from mobile devices, what percent (%) of these users are technically required to use two-factor PIV card authentication to access these resources and services?
0%

Physical Access Control Systems

- 3.9 Percent (%) of agency's operational Physical Access Control Systems (PACS) that comply with procurement requirements for purchasing products and services from the FIPS 201 Approval Products List maintained by General Services Administration (GSA) (per OMB M06-18).
65%

Comments:

Agency's FY14 response was based on policy. For FY15, 65% represents a percentage where the baseline is derived from all the facilities that require a FIPS 201 compliant PACS solution that electronically accepts and authenticates PIV credentials for routine access based on facility risk assessment. Where the baseline is derived from facilities that currently have PACS implemented that electronically accept and authenticate internal users' PIV credentials for routine access, the figure is 100%.

Section 3: Identity Credential and Access Management

- 3.10 Percent (%) of agency's operational PACS that electronically accept and authenticate internal users' PIV credentials for routine access in accordance with NIST standards and guidelines (e.g., FIPS 201-2 and NIST SP 800-116).

71%

Comments: 93% of Treasury facilities in the National Capital Region have this capability. These percentages are only indicative of the facilities that have a completed facility risk assessment and were determined must comply with NIST SP 800-116 for implementation of an electronic PIV-enabled PACS.

Section 4: Anti-Phishing and Malware Defense

- 4.1 Percent (%) of privileged user accounts that have a technical control preventing internet access.

97%

- 4.2 Percent (%) of incoming email traffic analyzed for clickable URLs, embedded content, and attachments.

99%

- 4.3 Percent (%) of hardware assets covered by a host-based intrusion prevention system.

65%

Comments: The Department has not yet achieved the 90% CAP target for this metric because in FY 2015 we elected to address Anti-Malware targets through implementation of anti-virus technologies and tools to block known phishing websites, as well as scanning remote access connections for malware upon connection.

- 4.4 Percent (%) of hardware assets covered by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information.

100%

- 4.5 Percent (%) of email attachments opened in sandboxed environment or detonation chamber.

35%

Comments: The Department has not yet achieved the 90% CAP target for this metric because the infrastructure supporting currently deployed email attachment sandboxing environments is not sufficient to analyze all email traffic.

- 4.6 Percent (%) of incoming emails using email sender authentication protocols such as DomainKeys Identified Mail (DKIM), Author Domain Signing Practices (ADSP), Domain-based Message Authentication, Reporting & Conformance (DMARC), Vouch by Reference (VBR), or IP Reverse (iprev).

88%

- 4.7 Percent (%) of incoming emails scanned using a reputation filter tool to perform threat assessment of email sender.

100%

Section 4: Anti-Phishing and Malware Defense

- 4.8 Percent (%) of hardware assets covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar).

4%

Comments:

The Department has not yet achieved the 90% CAP target for this metric in part because anti-exploitation features are currently only available for servers, workstations, and mobile devices, yet OMB requires this metric be calculated as a percentage of all network devices. Until the metric is appropriately scoped, 90% is not technically achievable.

- 4.9 Percent (%) of inbound email traffic passing through anti-phishing/anti-spam filtration technology at the outermost border Mail Transport Agent or email server.

99%

- 4.10 Percent (%) of inbound network traffic that passes through a web content filter that provides anti-phishing, anti-malware, and blocking of malicious websites (e.g., fake software updates, fake antivirus offers, and phishing offers).

100%

- 4.11 Percent (%) of hardware assets that have implemented a browser-based (e.g., Microsoft Phishing filter) or enterprise-based tool to block known phishing websites and IP addresses.

94%

- 4.12 Percent (%) of outbound communications traffic checked at the external boundaries to detect covert exfiltration of information.

100%

- 4.13 Percent (%) of sent email that is digitally signed.

70%

Comments:

The Department has not yet achieved the 90% CAP target for this metric because gateway email signing is currently enabled at only three of five TICs.

- 4.14 Percent (%) of email traffic quarantined or otherwise blocked.

92%

Section 5: Data Protection

223

Section 5: Data Protection

- 5.1 What is the estimated number of hardware assets in each of the following mobile and portable asset types, and how many are encrypted? Answer in the table below.

Mobile and Portable Device Types (each asset should be recorded no more than once in each column).	5.1.1 Estimated number of mobile hardware assets of the types indicated in each row.	5.1.2 Estimated number of assets from 5.1.1 with FIPS 140-2 compliant encryption of data on the device.
Laptop computers and netbooks	59199	54475
Tablet-type computers	386	317
Smartphones	13734	11091
Other mobile devices	656	455

Section 6: Network Defense

- 6.1 What is the estimated percent (%) of remote access connections that have each of the following properties:
- 6.1.1 Percent (%) that utilize FIPS 140-2-validated cryptographic modules.
100%
 - 6.1.2 Percent (%) that prohibit split tunneling and/or dual-connected remote hosts where the mobile device has two active connections.
100%
 - 6.1.3 Percent (%) configured in accordance with OMB M-07-16 to time-out after 30 minutes of inactivity (or less) and requires re-authentication to reestablish session.
100%
 - 6.1.4 Percent (%) scanned for malware upon connection.
99%

Section 7: Boundary Protection

Instruction: Questions 7.1 – 7.3 do not apply to the Department of Defense.

- 7.1 Percent (%) of the required TIC 2.0 Capabilities implemented.
99%

Questions 7.2–7.3 apply only to Federal civilian organizations. If the reporting organization is not a Federal civilian organization, answer N/A to these questions.

- 7.2 Percent (%) of external network traffic to/from the organization's networks that passes through a TIC/MTIPS.
99%

Section 7: Boundary Protection

- 7.3 Percent (%) of external network/application interconnections to/from the organization's networks that passes through a TIC/MTIPS.
93%
- 7.4 Percent (%) of public-facing servers use IPv6 (e.g., web servers, email servers, DNS servers, etc.). (Exclude low-impact networks, cloud servers, and Internet Service Provider (ISP) resources unless they require IPv6 to perform their business function.)
47%

Section 8: Training and Education

- 8.1 Percent (%) of users that successfully completed annual Cybersecurity Awareness and Training (CSAT).
98%
- 8.1.1 Percent (%) of new users who satisfactorily completed security awareness training before being granted network access or within an organizationally defined time limit that provides adequate security after being granted access.
96%
- 8.2 Percent (%) of all users that participated in cybersecurity-focused exercises.
5%
- 8.2.1 Percent (%) of the users in 8.2 that successfully completed exercises focusing on phishing, designed to increase awareness and/or measure effectiveness of previous training (e.g. organization conducts spoofed phishing emails, clicking link leads to phishing information page).
100%
- 8.3 Percent (%) of the organization's network users and other staff that have significant security responsibilities.
8%
- 8.3.1 Percent (%) of the personnel counted in question 8.3 that have successfully completing role-based security training within the reporting year.
99%

Section 9: Incident Response

- 9.1 Of the information security incidents reported to US-CERT in FY2015, what was the total number of incidents reported to Congress?
0
- 9.2 Of all of the cyber related (electronic) incidents with confirmed loss of confidentiality, integrity or availability reported to US-CERT in FY15 (per OMB M-15-01), what was the average mean time (in hours) between detection and notification to the Agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or Information Technology (IT) department?
1.0

Section 9: Incident Response	
9.3	When will the agency transition to the new US-CERT reporting format? 9/30/2015

Inspector General
Section Report

2015
ANNUAL
FISMA REPORT

DEPARTMENT OF THE TREASURY

For Official Use Only

For Official Use Only

Inspector General

Section Report

2015
Annual FISMA
Report

Department of the Treasury

For Official Use Only

Section 1: Continuous Monitoring Management

- 1.1 Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.
- 1.1.1 Please provide the D/A ISCM maturity level for the People domain.
Ad Hoc (Level 1)
- 1.1.2 Please provide the D/A ISCM maturity level for the Processes domain.
Ad Hoc (Level 1)
- 1.1.3 Please provide the D/A ISCM maturity level for the Technology domain
Ad Hoc (Level 1)
- 1.1.4 Please provide the D/A ISCM maturity level for the ISCM Program Overall.
Ad Hoc (Level 1)
- 1.2 Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.
N/A

Section 2: Configuration Management

- 2.1 Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
- No
- 2.1.1 Documented policies and procedures for configuration management.
Yes
- 2.1.2 Defined standard baseline configurations.
No

Comments:

Treasury OIG: DO has a self-identified weakness over baseline configurations for one of the selected systems. (See Self-Identified Weakness Section: POA&M #576 and #6149)

Section 2: Configuration Management**2.1.3 Assessments of compliance with baseline configurations.**

No

Comments:

Treasury OIG: Fiscal Service had a self-identified weakness over continuous monitoring testing was not conducted during the assessment period for one the selected systems. (See Self-Identified Weakness Section: POA&M #8393)

TIGTA: The IRS has not deployed automated mechanisms to centrally manage, apply, and verify baseline configuration settings and produce FISMA compliance reports using the NIST-defined Security Content Automation Protocol format for all of its information technology assets. The IRS is awaiting the outcome of the DHS's Continuous Diagnostics and Mitigation program Task Order #2 to provide the toolset to meet the program requirements.

2.1.4 Process for timely (as specified in organization policy or standards) remediation of scan result findings.

No

Comments:

TIGTA: The IRS has not yet fully implemented configuration baseline scanning tools and processes on all systems to ensure timely remediation of scan result deviations.

2.1.5 For Windows-based components, USGCB secure configuration settings are fully implemented (when available), and any deviations from USGCB baseline settings are fully documented.

Yes

2.1.6 Documented proposed or actual changes to hardware and software baseline configurations.

No

Comments:

TIGTA: The IRS has not yet fully implemented configuration and change management controls to ensure that proposed or actual changes to hardware and software configurations are documented and controlled.

2.1.7 Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI- 2).

No

Comments:

Treasury OIG: DO has a self-identified weakness over vulnerability scanning for one of the four selected systems. (See Self-Identified Weakness Section: POA&M #6736 and #7314)

TIGTA: The IRS has not implemented software assessment (scanning) on all systems.

232

Section 2: Configuration Management

- 2.1.8 Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2).

No

Comments:

Treasury OIG: DO has a self-identified weakness over configuration management and timely patching for two of the four selected systems. (See Self-Identified Weakness Section: POA&M #575, #578, #6861, #7788, #8631, and #8634) OCC has a self-identified weakness over configuration settings for the selected system. (See Self-Identified Weakness Section: POA&M #3741)
TIGTA: The IRS has not yet fully implemented configuration-related vulnerability scanning tools and processes on all systems to ensure timely remediation of scan result deviations.

- 2.1.9 Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 800-53: CM-3, SI-2).

No

Comments:

TIGTA: The IRS has not implemented a Service-wide process to ensure timely installation of software patches on all platforms.

- 2.2 Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.

See Comments

Comments:

Treasury OIG: DO has a self-identified weakness over audit logging capabilities for two of the four selected systems. (See Self-Identified Weakness Section: POA&M #7412, #7413, and #7645) Fiscal Service has a self-identified weakness over audit logging capabilities for one of the selected systems. (See Self-Identified Weakness Section: POA&M #3140 and #3141) OCC has a self-identified weakness over audit logging capabilities for the selected system. (See Self-Identified Weakness Section: POA&M #47)

- 2.3 Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability?

No

Comments:

TIGTA: The IRS does not have an enterprise deviation handling process that is integrated with the automated capability for all of its information technology assets. A number of its assessment activities involve manual processes.

STATEMENT SUBMITTED BY COMMITTEE RANKING MEMBER
EDDIE BERNICE JOHNSON

OPENING STATEMENT
Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
"Can the IRS Protect Taxpayers' Personal Information?"
April 14, 2016

I want to begin by welcoming the witnesses to today's hearing to discuss the need for stronger information security policies and procedures at the Internal Revenue Service in order to better protect taxpayers' personal information.

I am concerned about the identify theft that has already occurred and might yet occur because of weakness in information security controls at the IRS. Taxpayers have a right to expect that their information will be kept secure when they make use of online services provided by the Internal Revenue Service or any other government agency.

Congressional oversight of these matters is important. I expect that the many IRS hearings being held across Congress this week and next will help improve decision making for information security at the agency. However, I hope that these hearings will also help my colleagues improve Congressional decision making about funding for the Internal Revenue Service.

The Internal Revenue Service's budget has been cut by 17 percent since 2010, after adjusting for inflation, despite a 7 percent increase in the number of tax returns required to be processed, and despite new requirements under the Affordable Care Act and the Foreign Account Tax Compliance Act. These spending cuts, which triggered a 14 percent reduction in IRS employees, are a significant factor in weakened taxpayer services, reduced detection and enforcement of fraudulent claims, and the agency's ability to hire qualified staff needed to fulfill its many requirements under the Federal Information Security and Management Act. And if the House had its way in recent years, the agency's budget would have been cut even further.

So let us be critical of some of the management decisions made at the Internal Revenue Service with respect to protecting taxpayers' personal information. And let us be sure they are putting the people, systems, and processes in place to make better decisions going forward. But let us also be willing to provide the agency with the financial resources and other authorities they need to accomplish these goals.

Finally, cybersecurity is a big challenge that requires effective action by many people and offices at the Office of Management and Budget, the National Institute of Standards and Technology, the Department of Homeland Security, the individual implementing agency, such as the Internal Revenue Service, and their private sector partners. When agencies make poor decisions, we should hold them accountable. However, effective oversight will require more than just a hearing and a press release. If we are serious, this Committee will need to do the hard work of thinking

about better, smarter, more effective federal policies to help the agencies meet their information security goals and requirements.

Again, thank you to the witnesses for being here this morning, and I yield back.

