S. HRG. 114–580

CYBERSECURITY AND PROTECTING TAXPAYER INFORMATION

HEARING

BEFORE THE

COMMITTEE ON FINANCE
UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

APRIL 12, 2016

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PUBLISHING OFFICE

24–730—PDF 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 FINANCE

ORRIN G. HATCH, Utah, *Chairman*

CHUCK GRASSLEY, Iowa
MIKE CRAPO, Idaho
PAT ROBERTS, Kansas
MICHAEL B. ENZI, Wyoming
JOHN CORNYN, Texas
JOHN THUNE, South Dakota
RICHARD BURR, North Carolina
JOHNNY ISAKSON, Georgia
ROB PORTMAN, Ohio
PATRICK J. TOOMEY, Pennsylvania
DANIEL COATS, Indiana
DEAN HELLER, Nevada
TIM SCOTT, South Carolina

RON WYDEN, Oregon
CHARLES E. SCHUMER, New York
DEBBIE STABENOW, Michigan
MARIA CANTWELL, Washington
BILL NELSON, Florida
ROBERT MENENDEZ, New Jersey
THOMAS R. CARPER, Delaware
BENJAMIN L. CARDIN, Maryland
SHERROD BROWN, Ohio
MICHAEL F. BENNET, Colorado
ROBERT P. CASEY, Jr., Pennsylvania
MARK R. WARNER, Virginia

CHRIS CAMPBELL, *Staff Director*
JOSHUA SHEINKMAN, *Democratic Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL

COMMUNICATION

CYBERSECURITY AND PROTECTING TAXPAYER INFORMATION

TUESDAY, APRIL 12, 2016

U.S. SENATE,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 10:13 a.m., in room SD–215, Dirksen Senate Office Building, Hon. Orrin G. Hatch (chairman of the committee) presiding.

Present: Senators Grassley, Crapo, Thune, Portman, Coats, Heller, Scott, Wyden, Stabenow, Cantwell, Nelson, Carper, Cardin, Brown, Bennet, and Casey.

Also present: Republican Staff: Chris Armstrong, Deputy Chief Oversight Counsel; Eric Oman, Senior Policy Advisor for Tax and Accounting; and Mark Prater, Deputy Staff Director and Chief Tax Counsel. Democratic Staff: David Berick, Chief Investigator; Michael Evans, General Counsel; Daniel Goshorn, Investigative Counsel; and Tiffany Smith, Senior Tax Counsel.

OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM UTAH, CHAIRMAN, COMMITTEE ON FINANCE

The CHAIRMAN. The committee will come to order. I will mention that Senator Wyden is delayed. He will be here a little later. He has asked that I proceed without him, and we will be happy to have him participate when he comes.

Well, good morning. It is a pleasure to welcome everyone to today's hearing, which we have entitled, "Cybersecurity and Protecting Taxpayer Information."

Now, these are really important issues that the Finance Committee has been working on for some time. In June of last year, for example, we had a hearing on the theft of Internal Revenue Service data affecting taxpayer information. Much has happened since that time.

At the urging of the Finance Committee, the IRS, State revenue commissioners, and leaders in the tax return preparation industry came together last year to convene a Security Summit, which resulted in new information-sharing agreements to help identify suspicious activity in the tax filing and refund process. We look forward to hearing more about that effort today.

But in the face of this progress, we have also seen unprecedented growth in the scope and scale of cyber-attacks aimed at stealing personal information and billions of dollars from our taxpayers. Last year alone, cyber-criminals obtained access to sensitive personal information from several large health insurers, exposing tens

of millions of Americans to potential identity theft. Foreign governments gained access to poorly protected Federal Government databases, including a treasure trove of information at the Office of Personnel Management.

Today, we will focus on three separate aspects of this problem. First, we will consider the ways the IRS authenticates taxpayer identities to prevent data thieves from using authentication information to gain access to even more information about taxpayers or to file false returns and obtain refunds under stolen identities.

Second, we will examine how the IRS uses its resources to improve cybersecurity. This will include some discussion about the IRS Future State plan, which the agency has developed in order to adapt to the realities of the 21st century.

Third and finally, we will consider the ongoing joint efforts of the IRS, State revenue collectors, and private tax preparers to see what can be accomplished to better secure taxpayer information and protect taxpayers from fraud.

Taking a look at our witness table, it is clear that this is not a typical lineup of witnesses. Challenges to cybersecurity require not only smart and persistent leadership up at the top, but also technological expertise and up-to-date skills down on the ground.

So today, we not only have with us the heads of the IRS, the Government Accountability Office, and the Treasury Inspector General for Tax Administration, but we have invited subject matter experts on the relevant issues from each of those agencies to testify as well.

That is a total of six witnesses, and I suspect each of them will bring unique and important insights to this discussion.

In closing, I will just say that while we are clearly making real progress in this area, the challenges are continuing to grow and criminals behind this kind of data theft are getting more sophisticated and aggressive, seemingly by the day, and American taxpayers and their livelihoods are their targets.

In other words, we have a lot of work to do. My hope is that we will continue to be able to work on these issues on a bipartisan basis in order to do right by the American people.

Now, with that, I would like to turn it over to Senator Wyden, when he gets here, for any opening remarks he might have.

[The prepared statement of Chairman Hatch appears in the appendix.]

The CHAIRMAN. Our first witness will be John Koskinen, Commissioner of the IRS. We will start with you first, Mr. Koskinen, and go from there.

STATEMENT OF HON. JOHN KOSKINEN, COMMISSIONER, INTERNAL REVENUE SERVICE, WASHINGTON, DC; ACCOMPANIED BY TERENCE V. MILHOLLAND, CHIEF TECHNOLOGY OFFICER, INTERNAL REVENUE SERVICE, WASHINGTON, DC

Commissioner KOSKINEN. Good morning, Chairman Hatch, Ranking Member Wyden, and members of the committee. Thank you for the opportunity to discuss the IRS's ongoing efforts in regard to cybersecurity and identity theft. As the chairman noted, I am delighted to have Terry Milholland, our Chief Technology Officer,

here with me today for any specific technical questions you may have.

Securing our systems and taxpayer data continues to be a top priority for the IRS. Even with our constrained resources, we devote significant time and attention to this challenge. We work continuously to protect our main computer systems from cyber-attack and to safeguard taxpayer information stored in our database.

The systems withstand more than 1 million malicious attempts to access them each day. We are also continuing to battle the growing problem of stolen identity refund fraud. Over the past few years, we have made steady progress in protecting against fraudulent refund claims and criminally prosecuting those who engage in this crime, but we have found the type of criminal we are dealing with has changed.

The problem used to be random individuals filing a few dozen or a few hundred false tax returns at a time. Now, we are dealing more and more with organized crime syndicates here and in other countries. They are gathering, as the chairman noted, almost unimaginable amounts of personal data 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 leaders of the electronic tax industry, 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 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 have seen three examples of what identity thieves are capable of and why we cannot 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 was our Get Transcript online application, used by taxpayers to quickly obtain a copy of their prior year return.

Another was an online tool to retrieve a lost Identity Protection Personal Identification Number, or IP PIN. Taxpayers who previously were victims of identity theft use these PINs to prove their identity when they file a return.

The third was a tool that some people use to generate a PIN number when they e-file their tax return. In all three cases, criminals were trying to use our online tools to help them pretend to be legitimate taxpayers and sneak false returns past our fraud filters. These incidents, which, unfortunately, in the case of the Get Transcript access, resulted in the loss of taxpayer information for thousands of taxpayers before the applications were disabled, have shown us that improving our reaction time to suspicious activity is not 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 are 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 continuously upgrade and improve our ability to verify the identity of taxpayers using these services.

Taxpayers will only use these services if they are confident that they are safe and secure. So we are 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 online 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 for fiscal year 2016, which included funds to improve cybersecurity and fight identity theft. Sustaining and increasing funding in this area will be critical as we move forward.

Another way Congress helps 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 authority, 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 Hatch, Ranking Member Wyden, and members of the committee, this concludes my statement, and Mr. Milholland and I would be happy to take your questions.

[The prepared statement of Commissioner Koskinen appears in the appendix.]

The CHAIRMAN. Thank you so much.

Today's panel is a little bit unorthodox, at least as far as our typical hearings in this committee are concerned. In order to ensure that we have the most robust discussion possible—and I put that discussion into the record—we have invited the heads of three vital government offices to testify, as well as the subject matter experts in the relevant areas from each agency.

Now, we have heard from the first witness, John Koskinen, who has a tremendous reputation and background for the job that he is doing.

Our second witness will be Inspector General J. Russell George from the Treasury Inspector General for Tax Administration.

Mr. George was confirmed to his current position in November 2004. Prior to that, he served as the Inspector General of the Corporation for National and Community Services.

Mr. George began his career as a prosecutor in the Queens County District Attorney's Office in New York, following which he served as Assistant General Counsel in the Counsel's Office in the White House Office of Management and Budget.

Mr. George also has served as the Associate Director for Policy in the Office of National Service, after which he moved to the private sector, where he practiced law at Kramer, Levin, Naftalis, Nessen, Kamin, and Frankel.

Then in 1995, Mr. George returned to Washington, DC to join the Committee on Government Reform and Oversight as the Staff Director and Chief Counsel of the Government Management, Information, and Technology Subcommittee.

Mr. George received his bachelor of arts degree from Howard University and his law degree from Harvard University School of Law.

He will be joined by Deputy Inspector General for Audit, Michael McKenney. Mr. McKenney is responsible for providing audit oversight of IRS operations related to the preparation and processing of tax returns and the issuing of refunds to taxpayers.

Then finally, from the Government Accountability Office, we welcome back Comptroller General Gene Dodaro. Mr. Dodaro was confirmed as the eighth Comptroller General of the United States and head of the U.S. Government Accountability Office in December 2010. Mr. Dodaro was confirmed to this position after serving as the Acting Comptroller General since March 2008. Including these 7 years of dedicated service, Mr. Dodaro has served the country for more than 40 years at the GAO. He served most recently as the Chief Operating Officer and is also head of GAO's Accounting and Information Management Division, where he directed the first-ever audit of the comprehensive financial statements covering all Federal departments and agencies.

Mr. Dodaro has also worked closely with Congress in several administrations on major management reform initiatives, including the 1994 Government Management Reform Act, the revised 1995 Paperwork Reduction Act, and the Clinger-Cohen Act of 1996.

He received a bachelor's degree in accounting from Lycoming College in Pennsylvania.

Mr. Dodaro is joined by Information Security Issues Director Gregory Wilshusen, who leads cybersecurity and privacy-related studies and audits of the Federal Government.

I want to thank all of you for coming. I know that this is an expansive topic, and the more insight and perspective we can get, the better off we will be.

We will hear the witness testimonies in the order that I just introduced them.

Mr. George, we will turn to you at this time.

STATEMENT OF HON. J. RUSSELL GEORGE, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, DEPARTMENT OF THE TREASURY, WASHINGTON, DC; ACCOMPANIED BY MICHAEL E. McKENNEY, DEPUTY INSPECTOR GENERAL FOR AUDIT, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, DEPARTMENT OF THE TREASURY, WASHINGTON, DC

Mr. GEORGE. Thank you, Chairman Hatch, members of the committee, for the opportunity to testify today on the IRS's processes to protect sensitive taxpayer information.

As you noted, Mr. Chairman, I am joined by the Deputy Inspector General for Audit, Michael McKenney.

Cybersecurity threats against the Federal Government continue to grow, and the IRS is a very prime target for attacks because of

the extensive amount of taxpayer data it stores. As such, the security of taxpayer data is one of the top concerns facing the IRS.

TIGTA has identified a number of areas in which the IRS could better protect taxpayer data. For example, TIGTA recently reported that the IRS is working towards continuous monitoring of its overall information security posture. This effort will eventually allow the IRS to perform ongoing real-time assessments of information security so that it knows when and where security vulnerabilities exist.

We also reported that the IRS needs to fully implement unique user identification and authentication that complies with the Department of Homeland Security directives. Full implementation and integration of personal identity verification cards will help to ensure only authorized personnel can access computer systems and facilities.

Further, TIGTA has evaluated the effectiveness of the security patch management process. This process is key to mitigating the security risks associated with known vulnerabilities to computer systems. We found the IRS is still working to expand a standard automated process needed to ensure that all IRS systems are patched timely and are operating securely.

Web applications that provide online services are significantly vulnerable, because even without penetrating network security, hackers can and have cleared the authentication process to gain access to and steal valuable taxpayer information.

The IRS has established processes and procedures to authenticate individuals requesting online access to IRS services; however, these processes and procedures do not comply with government standards. For example, the processes that the IRS used to authenticate users of its Get Transcript and Identity Protection Personal Identification Number, IP PIN, applications, required only single-factor authentication.

Government standards require multi-factor authentication for such high-risk applications. Moreover, the authentication framework used for these applications did not comply with the government standards for a 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. To prevent further unauthorized access, the IRS removed the application from its website. Unfortunately, TIGTA's current 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.

We also reported in November 2015 that the IRS did not complete the required authentication risk assessment for its IP PIN application and recommended that the IRS not reactivate this application for the 2016 filing season. However, the IRS reactivated the application on January 19, 2016.

We issued a second recommendation to the IRS on February 24th, advising it to remove the IP PIN application from its public website. On March 7th, the IRS reported that it was temporarily

suspending use of the IP 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 IP PIN application to provide multifactor authentication capability before the summer of 2016.

The number and sophistication of threats to taxpayer information will likely continue to increase, and these threats will be a continued focus of our audit and investigative activity.

Chairman Hatch, Ranking Member Wyden, members of the committee, thank you for the opportunity to share my views.

[The prepared statement of Mr. George appears in the appendix.]

The CHAIRMAN. Thank you so much. We appreciate having your views.

We will now turn to Mr. Dodaro, and then I understand the other two witnesses will be here to answer questions, if necessary.

Mr. Dodaro, we will turn to you.

STATEMENT OF HON. GENE L. DODARO, COMPTROLLER GENERAL OF THE UNITED STATES, GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, DC; ACCOMPANIED BY GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, DC

Mr. DODARO. Thank you very much, Mr. Chairman. Good morning to you, Ranking Member Wyden, members of the committee.

Greg and I are very pleased to be here today to discuss GAO's work related to computer security at IRS and identity theft refund fraud.

Our most recent audit showed that IRS had instituted controls over its financial and tax processing systems. However, there were numerous weaknesses that we identified due to the inconsistent application of its information security program across IRS. These weaknesses included easily guessed passwords to gain access to servers supporting key systems at IRS, including those to access and manage taxpayer accounts, and users at the IRS who were given rights and privileges beyond what they needed to carry out their responsibilities, including access to electronic tax payment systems.

We found that key systems that should have been encrypted were not. We found in other cases there were applications where user activity was not being logged so that IRS could potentially investigate or know who was using those systems, including those that were used to transfer financial data and to manage and access taxpayer accounts. Also, we found that software patches were not being implemented in a timely fashion in a couple key instances.

Now, to address these weaknesses and strengthen IRS's security program, GAO made 45 new recommendations to the IRS. In addition, we reemphasized the importance of implementing 49 recommendations that we had made previously that were not yet implemented. One area we were concerned about with this most recent audit was that in 28 instances, IRS asserted that it had implemented our prior recommendations, but our subsequent testing showed that in nine of those 28 instances, the problem had not been fixed. So we are very concerned about that.

This included access by employees and visitors to one of IRS's computing facilities where access lists had not been updated as appropriate.

So we made many recommendations to strengthen IRS's computer security program. We are hopeful that IRS will rigorously implement our recommendations over the next few years, all 94 recommendations that we have outstanding.

Now, with regard to identity theft, I am very pleased to report that the Congress has acted on the recommendations that we had made to allow for more timely filing by employers of W–2 data.

As you recall, Mr. Chairman, I was here last year before this committee talking about the importance of providing earlier W–2 information to the IRS. In past years, IRS only received the W–2 information from employers in April. Having it earlier to match against early income tax filing will allow IRS to better detect tax returns that are filed using fake identities.

The new law now gives IRS the ability to have that W–2 information at the end of January. We think it is very important for IRS to implement changes to its processes and systems in order to take advantage of the new, earlier information.

We also think that IRS needs to continue to test and assess the costs, benefits, and risks of different authentication techniques that could be used. This has been a key weakness in the past on Get Transcript and the IP authorizations. IRS also needs to give better feedback to those who provide external leads to them, such as tips that they can follow up to further identify identity theft cases.

We also have a recommendation for the Congress. We think Congress should lower the requirement for electronic filing of W–2 data by employers from 250 employees down to a much lower number. This would give IRS more electronic information that it could use to match to help avoid identity theft in the future.

So, again, thank you for the opportunity to be here today. GAO is very committed to computer security in the Federal Government. We actually designated it as a high-risk area across the entire Federal Government in 1997. We have been working on it since then and made thousands of recommendations.

I am pleased to be here today to participate in this hearing, along with Mr. Wilshusen.

Thank you very much, Mr. Chairman.

[The prepared statement of Mr. Dodaro appears in the appendix.]

The CHAIRMAN. Thank you so much.

I want to apologize to Senator Wyden. I should have called on him right away, but we are going to call on him at this time.

OPENING STATEMENT OF HON. RON WYDEN, A U.S. SENATOR FROM OREGON

Senator WYDEN. Mr. Chairman, thank you. And to colleagues, my apologies for being late as well. I was at the public proceeding to look at steel overcapacity. We care a great deal about enforcing the trade laws on this committee, particularly the ENFORCE Act and the Leveling the Playing Field Act.

We are dealing with a steel overcapacity that would really cost us family-wage jobs, family-wage jobs in Oregon and across the country. We worked on this in a bipartisan way, and I was at the

USTR's proceeding to make sure that they move aggressively to enforce the law.

Now, we turn to the question of IRS cybersecurity, and it is pretty obvious that hackers and crooks, including many who work for foreign crime syndicates, are jumping at every opportunity to steal hard-earned money and sensitive personal data from American taxpayers. It happens online, and it happens in the real world.

In my view, taxpayers have been failed by the agencies, the companies, and the policymakers here in the Congress that they are counting on to protect them.

It was unacceptable for the IRS to leave the front door open to hackers by using a weak authentication process for its Get Transcript system. It meant that thieves could walk through the door and steal the tax information of three-quarters of a million taxpayers.

To make matters worse, after the IRS mailed the special Identity Protection PIN numbers to the hacking victims, it repeated its mistake and used lax security online. For the tax scammers, once again, it was as easy as going online, plugging in the personal data you have already stolen, and pretending to be somebody who lost their IP PIN.

So after leaving the front door open, the IRS left the back door open as well. There is simply no excuse for this.

But poor protection of taxpayer information is not just a problem at the IRS. There is plenty of blame to go around. Already this tax season, hackers have gotten into the inadequately guarded system of private software companies and stolen personal information from thousands of people. And it is my judgment that you cannot have an honest discussion about protecting taxpayer information without including the vulnerabilities from the e-file providers, as well as crooked return preparers who operate in the shadows and steal from customers.

For years, Republicans and Democrats have agreed on the need for minimum standards for return preparers, but the Congress has sat back and watched while criminals have come in and preyed on taxpayers. When it comes to blocking hackers, Congress has done next to nothing while the IRS loses its ability to hire the experts who can keep taxpayer information safe.

If you are a top-notch tech expert, you already are taking a pay cut to work in public service compared to what you would earn at firms in Oregon or California. Now, without what is called streamlined critical pay authority, it can take 4 to 6 months to bring a new hire on board at the IRS.

So I want to be clear as we go to questions. Taxpayer information is under assault every single day, but the IRS does not have the legal authority it needs from the Congress to build a cybersecurity team that can beat back the crooks.

Already there has been an exodus of high-ranking IRS tech staff. The Director of Cybersecurity Operations left 1 month ago. The terms for the remaining employees working under this authority continue to expire, including for one of our witnesses, Chief Technology Officer Terence Milholland. Come 2017, there are not going to be any left.

So today, instead of rehashing the past and just beating up on one agency or one firm, to me, the priority ought to be to focus on how to step up the fight against attackers and crooks across the board. It is my view that streamlined critical pay authority is a key part of the solution. There was a bipartisan bill, colleagues, ready to go last fall, and this committee ought to move forward on it as soon as possible.

Furthermore, the Congress needs to make more than token investments in IT at the IRS. Congress has held the IRS tech budget below where it was 6 years ago, but you can bet that the hackers have not backed down since then.

Next, the IRS and private firms need to do more to keep taxpayer information safe inside their systems. The Get Transcript hack I mentioned earlier has been well documented.

A recent audit by the Online Trust Alliance found that the security maintained by private free-file services did not meet expectations. It is unacceptable for troves of taxpayer data to be more vulnerable to hacking than many social media or e-mail accounts, and the committee ought to consider whether the IRS has the authority it needs to guarantee that the security used by private software firms is up to snuff.

While many tax preparers are honest practitioners, we know that there are always some bad apples in the barrel. Last year, Senator Cardin and I introduced a bill giving the IRS the authority to have basic minimum standards over these tax return preparers. We have worked to create a bipartisan identity theft bill for markup in the Finance Committee, which I had very much hoped would include at least these minimum standards for return preparers.

It is still my view that people handling sensitive taxpayer information should have to meet what are minimum standards and that the committee should vote to require it. Anybody who thinks that Western civilization is going to end if we have minimum standards can come to my home State, because we have them, and it is working well, and we heard testimony from a preparer that that was the case.

It is open season for hackers to steal money and data from hard-working Americans, so congressional inaction should not make this situation worse. With tax day approaching, millions of Americans are filing their returns online, through the mail, or with a private return preparer.

The committee has a responsibility to protect taxpayers, no matter what filing method they choose. So I see this hearing as an opportunity to find some bipartisan solutions to do what the Finance Committee has always done best, which is to find common ground.

I thank our witnesses, Mr. Chairman, and I look forward to working with you and our colleagues.

[The prepared statement of Senator Wyden appears in the appendix.]

The CHAIRMAN. Thank you, Senator. I appreciate it.

Let me begin by asking this. The IRS is working with State revenue commissioners and the private tax industry in the so-called Security Summit and has made an agreement to create an information-sharing and analysis center, or ISAC, to facilitate the sharing

of actionable information to prevent refund fraud and identity theft.

Now, I understand the agency has made progress on this, but it remains incomplete. It hope that it moves forward as quickly as possible.

I have two questions for the IRS and anyone else who would care to comment.

One, when do you anticipate the ISAC will be up and running? What impediments are delaying its launch?

Mr. Commissioner, given that we are nearing the end of the 2016 tax filing season, describe the extent to which the IRS and its partners are currently sharing information to prevent stolen identity refund fraud and how you measure whether that is working or not.

Commissioner KOSKINEN. Thank you, Mr. Chairman.

The Security Summit has been thus far a great success. In fact, part of the indication of its success is that the private-sector members have requested, which we have honored, that we make it a permanent partnership going forward, because it has already demonstrated its great utility.

We have been able to receive information from State tax commissioners, as well as preparers, about suspicious patterns. We have been able to exchange information, give them notice when we see suspicious patterns or Social Security numbers that have been abused, and we have been able to share that information in real time with the private sector and with State tax preparers.

As you noted, we agreed early on that an information-sharing center would be very helpful to increase the utility of that information and its availability.

I would stress the private sector and the IRS and the States are all protective of individual taxpayer information, so the information we are sharing is about patterns, it is about activities going on; but basically, we are not sharing individual taxpayer information, except in situations where we know there have been fraudulent attempts to access those accounts.

We measure it. Thus far, we have had a significant increase in the amount of leads provided. We have had a significant increase in the volume of refund fraud stopped. We have stopped over a million tax returns this year that were suspicious. We identified thousands of them that were fraudulent.

We have shared all that information back and forth. We do think that as soon as we can, we will try to implement the ISAC. It will take some time for this unique opportunity. We are funding it with some of the money that we were given out of the $290 million the Congress provided us additionally this year. Some of it is going, in fact, to the development of the ISAC.

We hope to have it up and running as soon as we can. It is not clear that we will be able to get it fully operational by next tax season, but I would stress that we are already exchanging information back and forth in real time, and it has been very helpful.

The CHAIRMAN. Thank you. This is a question for all of the witnesses regarding unimplemented recommendations related to information technology, cybersecurity, and identity theft.

In a report released last month on IRS information security, GAO identified specific IRS vulnerabilities that leave the sensitive

taxpayer information of millions of Americans "unnecessarily vulnerable to inappropriate and undetected use, modification, or disclosure." GAO made 45 new recommendations on how to better protect this data and identified 49 prior information security recommendations that the IRS has failed to implement.

Last year, Chairman Brady, Senator Rubio, Congressman Yoho, and I wrote to the IRS requesting an update on TIGTA recommendations relevant to today's hearing, and I was disappointed to learn that several continue to remain unimplemented.

I would just like to ask both TIGTA and GAO to detail the recommendations that you deem most important and discuss whether incidents like the unauthorized access of the Identity Protection Personal Identification Number tool would have occurred had these recommendations been implemented.

I would also ask the IRS to respond to the status of these recommendations.

Mr. GEORGE. Mr. Chairman, as it relates to the latter point, we believe that if our recommendations had been implemented, while we could not guarantee that the breach would not have occurred, it would have been much more difficult for that to have happened.

But I would like to defer to my colleague, Michael McKenney, for the additional response.

Mr. MCKENNEY. One thing, especially in the area of authentication, that is probably one of the more important recommendations to improve its authentication, is to move to the multi-factor authentication.

There are also some concerns we have expressed in the past that I think are really primary here, such as the IRS's willingness to accept risks in these areas without really very well following a process to document why they have accepted those risks and the rationale for what they have done to mitigate those risks.

So one of the most significant concerns we have is the agency itself, when it decides to accept risk. It is unavoidable, but it should be kept to a minimum, and when they do accept risk, they should thoroughly document why, the rationale, and what they will eventually be able to do to overcome those risks.

The CHAIRMAN. Senator Wyden, we will turn to you now for your questions.

Senator WYDEN. Thank you very much, Mr. Chairman.

Commissioner Koskinen, it seems to me you do not fight the cheats and the rip-off artists by osmosis. You do it by having the right kind of experts, the talent that you need to take them on.

Many of those experts were hired using streamlined critical pay, including the head IRS official who is sitting next to you, Mr. Milholland. But that authority expired in 2013, and the IRS has already lost many of these experts.

I think it would be very helpful if you laid out for the committee what are going to be the consequences of the Congress failing to renew this key tool, the streamlined critical pay authority, so you can go out there and get people who know how to beat the crooks.

Commissioner KOSKINEN. Well, we are concerned about it. That is the reason I have been talking about it for the last 2½ years, because what it gives us is the ability to find top-notch IT people and hire them, with suitable background checks, without going

through the 3- to 6-month normal government application process—and these are all highly desirable people.

Our people are being recruited every day, and when you tell somebody, "We would love to hire you; we have a great position for you; now, if you will just sit around for 3 to 6 months, we will get back to you and, in the meantime, fill out the applications and apply for the job," needless to say, most of those people are not around when we come back.

Now, there are good people who are willing to work through that process, but at the top of the heap, cybersecurity experts, people expert at development of new techniques and technologies, like Mr. Milholland, they simply do not need to go through that entire process.

So authority was provided in the Restructuring Act of 1998, was renewed every 4 years, and the IG reviewed the program a year and a half ago and found that we had used it appropriately. It only applies to 40 slots, and we never used the full 40.

But if we continue to lose people—we have 10 last IT people on the list—and by this time next year, they will all be gone, and our ability to replace them is very questionable.

Senator WYDEN. All right. Inspector George, we always value your work. I gather that you all have looked at this issue as well, and you largely agree with what the Commissioner has said, that these were justifiable hires, that these are exceptionally well-qualified individuals, and that this was something that really worked.

Is that true?

Mr. GEORGE. It is true, and it was actually even under budget. This is one of the programs implemented by the IRS that we have to say works. It is very successful and justified.

Senator WYDEN. I am going to repeat that for my colleagues. So here we have something that has been an essential tool. We are not going to have it any longer absent Congress getting serious on a bipartisan basis to renew it. And Inspector George, whose views we have long admired on both sides of the aisle, said the program came in under budget.

I appreciate your doing that, Inspector, because if that is not a wakeup call to the Congress, I do not know what is. This is something that works, and if we are going to beat the crooks, we ought to have it.

Now, Commissioner Koskinen, let me ask you about the private e-file providers, because I think we all understand that the IRS is not the only place where the bad guys, the crooks, can go after innocent taxpayers.

In January, two e-file providers revealed that roughly 16,000 taxpayer accounts had been breached. The Independent Online Trust Alliance concluded that 6 of 13 private online free-file tax preparation services failed the best practice assessment with respect to these cybersecurity tests.

Are e-file providers doing enough to keep taxpayer information safe, and, in your view, what needs to be done on this issue—again, with the Finance Committee, Democrats and Republicans, working together to ensure that we are using the tools that are essential.

Commissioner KOSKINEN. That is an important question. One of the great outcomes of the Security Summit, the partnership we have with the private sector, is from the start, in our meetings with them, all of the preparers and providers and software developers agreed that they would all meet the NIST standards of operation. Most of them already met them.

So it has not been a question of our having to require it. They have actually voluntarily agreed to a standard system of security, and they have gone beyond that. They have agreed to standard authentication procedures for taxpayers who use their services.

So it is one of the great examples of what happens if you have a public-private partnership where both sides are working together to solve a problem. You can make great progress, and we feel comfortable that our partners in the private sector see this as an important problem. They want to protect their clients. None of them wants to have a breach. And they have all been willing to work cooperatively with us to set appropriate standards and agree to them.

Senator WYDEN. So the last leg of this game plan, in addition to critical pay authority and the tools to deal with these e-file rip-offs, is tax preparers.

Once again, Chairman Hatch and I have had bipartisan legislation on this ready to go, and, for the life of me, I cannot understand, when taxpayers are ripped off, why we cannot have minimum standards.

Where you all are sitting, we had a witness from Oregon who made it very clear the sky is not going to fall, Western civilization is not going to end, if we have minimum standards.

I just want to wrap up with a question for Mr. Koskinen and Mr. Dodaro, whose work we also have long appreciated.

My understanding is, you both think that there should be minimum standards over preparers based on what you have seen over the years, with all the problems that stem from the fact that, while most preparers are honest and reputable business leaders, we, unfortunately, have some bad apples.

So is that your judgment, gentlemen, that there need to be some minimum standards over these preparers?

Mr. DODARO. Yes, Senator Wyden, I believe that. We have recommended that Congress give IRS the authority to regulate paid tax preparers, and I say that for several reasons.

One, we did an undercover investigation that sent teams out to 19 paid tax preparers. Only two of the 19 paid tax preparers gave us correct answers, and some were very wrong.

We also looked at 3 years of data at that time and found that paid tax preparers made errors 60 percent of the time versus 50 percent of the time for taxpayers who filed on their own behalf.

IRS found that paid tax preparers file about 68 percent of the Earned Income Tax Credit returns in a 1-year or 2-year period of time, and about 48 to 53 percent of those returns over-claimed the tax credit.

I definitely think there needs to be authority given IRS to set minimum standards for paid tax preparers.

I would also comment that we think the IRS should have more monitoring and oversight of the security and privacy standards

that paid tax preparers agree to use. We have had an open recommendation in this area since 2009.

Senator WYDEN. Thank you for your professional work.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

I would just say we have heard a lot today from the IRS and the ranking member regarding streamlined critical pay authority.

As Senator Wyden noted, re-implementing this authority is included in a bipartisan bill the committee introduced last year, and we will be moving to consider this particular bill in the near future. So hopefully we can resolve some of these problems.

Senator Grassley, we will turn to you.

Senator GRASSLEY. I am going to start with Director Wilshusen, please. I spent a little time comparing your 2015–2016 reports on information security at the IRS. Let me take a couple of examples.

In 2015, one specific observation was that on two databases, account passwords were not set to expire every 90 days, as they should be.

In 2016, the report says two of the 13 databases reviewed again had passwords that did not expire every 90 days, as they should have.

Do you know if these were the same two databases?

Mr. WILSHUSEN. Yes, sir, they were.

Senator GRASSLEY. It is common to hear that the lack of funding is why we cannot have better cybersecurity. So I might ask you, what is the approximate cost of setting up a password to expire every 90 days?

Mr. WILSHUSEN. It would be negligible, sir. It would not be a high-cost issue. It would be very low-cost, indeed.

Senator GRASSLEY. Again, both the 2015 and 2016 reports had a section dedicated to physical access control procedures that were not consistently implemented. The 2016 report observes that security guards control physical access to each IRS computing center.

Quoting now from the 2016 report, quote, "IRS has yet to address weaknesses pertaining to its review of its authorized access lists to sensitive areas for both employees and visitors at one of its computing centers."

So it is not an either/or. But I wonder if you could compare the cost of a dedicated guard force to the cost of reviewing a list of people who appropriately have access to the facility.

Mr. WILSHUSEN. Well, certainly, employing and deploying a guard force would cost significantly more than what it would to just review an access list on a periodic basis. That would be basically very low-cost, and it is something that should be done as a normal course of business.

Senator GRASSLEY. Your 2015 report found the agency did not always ensure that contractors received security awareness training within 5 business days, as required.

The 2016 report found the same problem and noted that the IRS acknowledged it had not addressed the issue.

Could you say if this contractor problem is that they get the training, but that they get it late, or do they just not get it at all?

Then I will follow that up right now. How expensive would it be to get the training in a timely manner rather than late?

Mr. WILSHUSEN. Well, first of all, it is that they do not receive it in a timely manner. The contractors do not receive this training, for the most part, in a timely manner.

And in terms of cost, if it is a web-based training, it should not cost much additional money to ensure that they receive it within the 5 days of gaining access to IRS systems.

Senator GRASSLEY. A couple of questions about mainframe security policy. Both your 2015 and 2016 reports say that, according to the mainframe manufacturer, policy should address who can administer the security software configurations that control access to mainframe programs.

Is that correct?

Mr. WILSHUSEN. Yes, sir.

Senator GRASSLEY. And both reports indicate that the IRS mainframe security policy does not address who can administer these configurations. Is that correct?

Mr. WILSHUSEN. Yes, sir.

Senator GRASSLEY. What would be the cost of naming the person or persons who can administer the software configurations that control access to mainframe programs?

Mr. WILSHUSEN. There should really not be much of any cost associated with that. It is just an assignment of responsibilities that IRS should make to assure that those individuals have been designated and take the appropriate steps to limit access as appropriate to those mainframes.

Senator GRASSLEY. So I would like to ask, Commissioner Koskinen, as you heard me ask Mr. Wilshusen about findings and recommendations that appear over and over in the GAO report—or at least each of the last 2 years—about cybersecurity at your agency, I took special note of four areas: setting passwords to expire every 90 days; two, a monthly review of lists of who should have access to computer centers; three, timely security awareness training for contractors; and, fourthly, the naming of administrators for software security on mainframe programs.

Would you agree that these are low-cost changes that could improve cybersecurity, and if they are, then why have they not been done?

Commissioner KOSKINEN. They are low-cost. I would note that we value highly both the reports and recommendations from GAO and from the IG, particularly in cybersecurity areas.

In the last several years, we have counted up over 2,000 GAO recommendations, of which we have already implemented about 80 percent.

In the internal security—and these are important internal security issues, not external, but they could become external, obviously—one of the things we are moving toward in terms of access is that passwords themselves turn out to be somewhat questionable, and we are moving toward what we call PIC cards, where you can actually only access servers—right now, you can only access e-mail with a Personal Identity Card you put into the computer.

We are moving toward having that be the system for access to all servers, all mainframes, and security online, so that it does not matter if you have given away your password or somebody seeks it, they will not be able to have access without the card.

But I agree, to the extent we can—we have a wide range and a large number of recommendations from both the IG and GAO. We do not disagree with those. We are working as quickly as we can to implement them, and these are particular ones internally to make sure that—we worry a lot about external threats. We also need to worry about internal threats, inadvertent or otherwise, and that is a high priority for us.

Senator GRASSLEY. Then I would expect that these will not be in the 2017 report.

Commissioner KOSKINEN. I can almost guarantee you, working with GAO, they will not be. But GAO, I would note, has done a very important thing for us. Out of their range of recommendations, they have given us their priorities or what they think are the highest priority for us to do.

Because there are limitations of time and resources, the ability to identify which of the recommendations have the highest priority is very helpful to us, and GAO has been very good about giving us that guidance.

Senator GRASSLEY. Thank you.

The CHAIRMAN. Thank you, Senator.

Senator Carper?

Senator CARPER. Thanks, Mr. Chairman.

I want to associate myself with the comments of Senator Wyden earlier. I thought he nailed it with his comments with respect to the streamlined critical pay program. Mr. Chairman, you mentioned in your comments that legislation had been introduced, bipartisan legislation was introduced last Congress. I just think it is critical that we follow through on that.

Year after year, Mr. Koskinen and others come to us and say, "Please do this to enable us to do our jobs more effectively," and a lot of times we point the finger at them and say, "You know, you screw up here and you screw up there, your people have as well." We have some responsibilities in this too, and one of the things that we could do to help out is to provide for the reestablishment of the streamlined critical pay program.

Mr. Chairman, you are going to hear a lot from me in the months to come, saying we should do this, let us do it, let us get it done. We need to do our job. We need to do our job.

We hear a lot about that lately. We need to do our job. This is another area where we need to do our job.

Mr. Dodaro, I want to ask you—I want to come back to this other point that Senator Wyden raised, and that is the minimum standards for paid tax preparers.

Would you just give—I think you guys have looked at this before, you folks have looked at this before. Just give us a minute or so on what we should be doing in this regard.

Mr. DODARO. We made a recommendation several years ago that IRS institute regulations over paid tax preparers, which it did, and then those regulations were overturned by the court because it viewed that IRS did not have statutory authority to do this.

As I mentioned earlier, our work has consistently shown that there are problems with some paid tax preparers. We sent teams of people to 19 paid tax preparers. We checked in advance with the IRS what the right answers should be to our tax scenarios. Only

two of the 19 paid tax preparers gave us correct answers. Some were very far off, to the point where they could have resulted in penalties and interest, both for themselves as well as for the people whom they were filing for.

We also looked at IRS data, at a 3-year period of time, and found that paid tax preparers made errors 60 percent of the time versus 50 percent of the time for taxpayers filing on their own behalf.

Senator CARPER. It was actually worse.

Mr. DODARO. Yes. Yes.

Senator CARPER. What should we do?

Mr. DODARO. Well, I think you need to give the IRS the authority, the statutory authority, to regulate paid tax preparers. They need to set minimum standards. They should go through a due process procedure just as you would with any regulatory approach and set the standards and enforce those standards.

This is a particular problem because of IRS's resource levels. If the government is going to rely on paid tax preparers to largely carry out a very important function on behalf of the government, then it needs to make sure that they are properly carrying out their responsibilities. IRS could greatly leverage the preparers' activities as opposed to a need to continually beef up the IRS.

Senator CARPER. Thanks so much.

Last year, Mr. Koskinen, I worked with a number of our colleagues, some on the Homeland Security and Governmental Affairs Committee, some on the Intelligence Committee, and others, to eventually pass the Federal Cybersecurity Enhancement Act of 2015. Among other things, the bill strengthened an important cybersecurity system at the Department of Homeland Security that is known as EINSTEIN 3A. The EINSTEIN program uses the best threat intelligence from our national security agencies to block cyber-threats before they can actually reach our Federal agencies in many instances.

It is my understanding that EINSTEIN 3A is now available to all Federal agencies. However, not all agencies, including the IRS, are signed up for EINSTEIN 3A.

The bill we passed last year also made participation in the program mandatory for all Federal civilian agencies.

When will the IRS adopt EINSTEIN 3A and start receiving its protections?

Commissioner KOSKINEN. I would like to give you Mr. Milholland.

Senator CARPER. Mr. Milholland?

Mr. MILHOLLAND. We are very familiar with the EINSTEIN program, 1 and 2, and we are scheduled to receive the EINSTEIN 3 equipment this year, and then there is the issue of implementing it.

So certainly by next filing season, I suspect that we will have it all done.

Senator CARPER. So by next filing season, like a year from now?

Mr. MILHOLLAND. Yes, sir. As I say, we have to schedule ourselves with DHS to receive the equipment, install it, test it, and then implement it. It is not something that is done overnight.

Senator CARPER. That is a lot of nights. We have 365 nights.

Mr. MILHOLLAND. Again, we are not yet scheduled from DHS. So it is something we have to work out with another agency as to when we actually get the equipment.

Senator CARPER. We are going to go to work on that and make sure that we do everything we can to move you up in the queue.

Mr. MILHOLLAND. Thank you, sir.

Senator CARPER. You bet. Thanks so much.

Thanks, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

Senator Scott?

Senator SCOTT. Thank you, Mr. Chairman.

Good morning to the panel and thank you for taking the time to be here, and we certainly appreciate your investment of time and your energies toward making sure that taxpayers' information is secure as possible.

I certainly know firsthand that identity theft is a terrifying experience and one that we should all hope that all taxpayers have an opportunity to avoid. The reality of it is that what we have seen over the last several years is too many taxpayers having too much information exposed inappropriately and, frankly, very poor results.

Unfortunately, there seems to be a systemic failure at the IRS in protecting taxpayer information, despite repeated warnings that the IRS needed to strengthen and modernize protection of taxpayer information. Due to these failures, I have received a number of e-mails from constituents throughout South Carolina, one in the last couple of days specifically from a taxpayer in Lexington, SC, who seems just bewildered at what the Federal Government, particularly the IRS, is doing to protect personal information.

I am interested in learning more about what the IRS is doing, and we certainly have heard a number of presentations and a lot of information about some programs that would be successful.

Other than what has already been mentioned, what else do you think should be done and can be done? If you can take maybe 50 seconds to answer that one.

Commissioner KOSKINEN. We are doing a wide range of things. One is, we are getting ready to establish a significantly increased authentication protocol. It will mean more taxpayers will not be able to answer the questions or get in, but it will make the system more secure.

As noted, we are moving to protect the systems with PIC cards, so people can only access e-mails or servers with personal identity cards.

We are working, and the private sector is working very closely with us—and we have a public relations campaign going with them out to taxpayers, trying to give them information on how to protect their data.

I would stress the accesses that have been obtained at the IRS were by criminals able to masquerade as taxpayers because they already had the information on the taxpayers.

So we think it is important for individuals to be careful what they do with their information, not to give out their Social Security numbers, not to use the same user ID and passwords all across the board, because we are all in it together.

Senator SCOTT. Thank you very much. Another issue that we have had many conversations about, and certainly one that I think should be deeply troubling to all of us, is the ruling last month by the Sixth Circuit Court that basically, in *United States v. NorCal Tea Party Patriots,* demanded that the IRS stop their games of delaying and turn over the documents requested by the plaintiffs.

In fact, the Sixth Circuit called the conduct displayed by the IRS attorneys outside the tradition of defending the Nation's interests in enforcing its laws. And while we spend a lot of time on cyberbreaches, the reality of it is that protecting all taxpayers should be one of our top priorities.

Has the IRS complied with that court order?

Commissioner KOSKINEN. We have complied with that court order. We have given the plaintiffs the information they requested, the names and addresses of the organizations.

As you know, our strong view was, that was taxpayer information. We have a lot of applications for a lot of things, whether it is private letter rulings or applications to become a c(3), (4), (5), (6), or (7), and oftentimes people, when they apply, do not assume that the application will be made public.

So we disagreed with the court, but we have complied with the court, because we have that order, but we have only complied with the information specifically in that case, and we have only done it in that case. We have not made a decision about any other case.

Senator SCOTT. Thank you.

The CHAIRMAN. Senator Coats, you are next.

Senator COATS. Thank you, Mr. Chairman.

I would like to direct my question to Mr. George. Mr. George, I raised the issue of employment-related identity theft with the Commissioner the last time he testified before the committee here, and I know that TIGTA has done a lot of work on this issue.

These are cases in which someone uses someone else's identity, their name or their Social Security number, to get a job illegally, on the employment side. A W–2 form with this false information is then sent to IRS and the Social Security Administration by an employer, or the W–2 may be attached to the tax return of the undocumented worker.

Our staffs met to try to work this out. It was a couple of months ago. What we learned is that, one, the IRS continues to process tax returns with false W–2 information and issues refunds as if they were routine tax returns, saying, "That is not really our job; we are there to process the returns and issue the refunds or collect what is overdue."

We also learned the IRS ignores notifications from the Social Security Administration that a name does not match a Social Security number, and you use your own system to determine whether or not a number is valid.

We learned that employers are liable for IRS fines and penalties if they submit false W–2 information, yet neither the IRS nor SSA is notifying employers that the information they are submitting is false.

We learned that IRS identified 200,000 new cases of employment-related identity theft last year and marked victims' accounts, yet did not notify the victims, again, saying, "That is really not our

job." In fact, the IRS forbids its employees from notifying victims that their information has been stolen. The IRS does not examine returns submitted on paper for employment-related identity theft.

Lastly, we learned that when the IRS marks the account of a victim, it does not notify the Social Security Administration that the victims did not earn the income reported on the W–2, and, as a result, the victims could lose income-related benefits because their Social Security earnings are not corrected.

My question to you is, one, have we made some progress since we met, on the basis of what we learned; and secondly, if you do not have the authority to better inform victims or connect with SSA on the potential fraud and notify each other, do you need authority to be able to do that? Do you need a statutory mandate here from the Congress to do that? Where do we go from here?

I think all of us can agree that victims need to know that they are victims, and they need to know that an agency of the Federal Government, whether it is IRS or whether it is SSA, or both, ought to have some ability to talk to each other to make sure that they do not run afoul of one or the other.

I am happy to hear your response.

Mr. GEORGE. Thank you, Senator. What you stated at the outset of your question is completely accurate.

I would note the IRS did have a pilot program to address this issue. That program ended. So they are not providing the information that you pointed out, but we are literally, sir, in the process now of assessing this overall issue and expect to issue our report in June of this year.

Senator COATS. Well, I am glad to hear that, but was the pilot program false? I mean, it just did not work out, is that——

Mr. GEORGE. I will defer to the Commissioner to describe whether or not he thinks it was—was it false? No, but they made a decision not to continue it, and I do not know whether it was resource-driven or what factors they took into consideration, Senator.

Senator COATS. Commissioner, I would be happy to have your response.

Commissioner KOSKINEN. Surely. Again, as you know, what happens in these situations is, someone is using a Social Security number to get a job, but they are filing their tax return with their ITIN—they are undocumented aliens. And so on that ground, they file taxes. It is in everybody's interest to have them pay the taxes they owe.

The question is whether the Social Security number they are using to get the job has been stolen, though it is not the normal identity theft situation. We did run a pilot, and we are looking at—and I appreciated your discussions about this—whether there is a way we could simply advise people.

A lot of times, those Social Security numbers are, in fact, borrowed from friends or acquaintances, and people know they have been used. Other times, they do not.

So we are looking at—and one of the reasons for the pilot was—what is the most effective way to deal with this without necessarily having people decide not to file their taxes—obviously a priority for taxpayers and the IRS, which is collecting those taxes.

So I would be delighted to have us get back to you with more detail on exactly where we are. And in some cases, there may be a need for statutory authority, and we are very sensitive about protecting taxpayer information on both sides.

But we will be delighted to give you the update on what we have learned and what we might be able to do going forward.

Senator COATS. Mr. George?

Mr. GEORGE. Thank you, Senator. I just wanted to add that there was a bill introduced entitled the Social Security Identity Defense Act that would require the IRS to inform an individual whether their SS number has been fraudulently used. I do not know where it stands now in terms of the legislative process.

Senator COATS. Well, we can check that out.

Commissioner KOSKINEN. But I would note specifically, we do advise taxpayers, when there has been any kind of access to one of our online applications, that their Social Security number is in the hands of criminals.

What we are talking about here is a very limited case of people filing taxes with an ITIN, but it is clear that they used the Social Security number to get the job.

But in all the other cases, we have sent out hundreds of thousands of letters, even when our system has not been accessed, warning taxpayers, no information was obtained from us, but you should know criminals have your Social Security number and other identifiers, so you should take whatever actions you can to protect that information.

Senator COATS. If I could, Mr. Chairman, just one last question.

My tax preparer, by the way, who is fully certified, just sent me an e-mail asking would I prefer to have my tax returns filed electronically or by paper. How am I safer—which way?

Commissioner KOSKINEN. You are actually safer electronically, because we can mark accounts. The only difference is, when you file on paper, it just takes longer to process, takes longer to get a refund.

We get fraudulent paper returns. So it is not as if the criminals do not file paper as well.

So we encourage everyone to e-file. Over 86 percent filed last year electronically, and as noted, it does give us the ability to track patterns more easily, and it is part of the data we share with the private sector and the States.

So our advice to you is, file electronically.

Senator COATS. Any other answer would probably flood your agency with a lot of paper. [Laughter.]

I will put that in that context. Anyway, I ended up doing it electronically. I hope it works.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

Senator Cardin, you are next.

Senator CARDIN. Thank you, Mr. Chairman. I thank all of our witnesses today in regards to the integrity of the system.

We are very concerned about the recent warning that was given to Maryland, Virginia, and DC taxpayers, due to the phishing scams, trying to trick victims into verifying the last four digits of their IRS number in order to get unsuspecting taxpayers' informa-

tion that can be used to compromise their privacy and their financial integrity.

I guess I will go with the Commissioner. Could you just update us as to the status of that particular concern and whether there should still be high alert in our region in regard to this scam?

Commissioner KOSKINEN. I think there should be. One of the things I think everyone should be aware of is—people should be aware of all the possible scams out there. There are the phone scams, where people call you and pretend to be from the IRS and threaten you, and we keep telling people, if you are surprised to be hearing from us, you are not hearing from us, and you should report that call. We work with the IG very closely on that.

There are phishing expeditions of all kinds, from masquerading as coming from financial institutions to the IRS seeking information or personal information. A lot of times you will get a note that says your account is frozen, click here and you can unfreeze your account. You should never do that. No bank or financial institution will put you through that system.

So this one is the most recent. We have had a couple new ones this year. We have had private-sector companies, where it would appear to be an e-mail from the CEO asking for personal information about employees, but it turns out to be an e-mail that is a phishing expedition from criminals.

So in this area, we are encouraging people to always remember that no one is asking legitimately for any personal information like Social Security numbers online or on the phone, and so you should not either click on the link and you should not provide that information.

Senator CARDIN. Do you know why this has been geographically in this region that this particular scam is being used?

Commissioner KOSKINEN. We do not. We know ID theft began, kind of flourished in Florida. We have a pilot program for IP PINs that has run for a couple of years in Florida, Georgia, and the District of Columbia.

Why those were the three areas where we have had more identity theft is hard to know, but the District has always been one of the areas that has been most prone to identity theft. And so it is not unusual for a permutation on that scam or scheme to happen in the same geographic area, but there is no other indication.

We cannot even tell you why the District of Columbia and Georgia are on the high end of identity theft. It just turns out to be one of those things that develops.

Senator CARDIN. One of the challenges in this environment is that we have to use all the resources we have at our disposal. That is, the Federal agencies need to work with the States and need to work with private entities and need to work with taxpayers.

What efforts are underway to try to coordinate the resources to go after those who are committing these frauds?

Commissioner KOSKINEN. We have a great effort—as I say, we work very closely with TIGTA. They have been tracking down people who are participating in phone scams. We have prosecuted and thrown in jail about 2,000 people for identity theft. We have about 1,700 investigations going on right now. We work closely with the Department of Justice in those areas.

In more general phishing expeditions, they are harder to track down. We work with the Federal Trade Commission and others to make sure that that information is readily available to the public.

As I said, the partnership we created a year ago with the private sector and the States has been a great vehicle for us, not only exchanging information about taxpayers, but exchanging information about fraud.

We learned about the private-sector company CEO e-mail from one of our partners, and what has happened is, we all then can publicize that and put it out.

So it is, I think, a significant step forward, but your point is well taken. We need everybody working together on this matter. As I told the States and the private sector when we brought them together, it is clear no one of us by ourselves is going to be able to successfully deal with this problem.

Senator CARDIN. Mr. George, do you want to respond?

Mr. GEORGE. Senator, just to give you a sense, as of this week, we at TIGTA received approximately 1.2 million calls concerning impersonation cases, with approximately $31 million having been sent by people in scams.

So as the Commissioner noted, we at TIGTA have engaged in public service announcements. We are doing as much local media as possible. The key is getting the word out, and you would be shocked how difficult it is sometimes to convince people that, as the Commissioner indicated, if you do not think you have an IRS problem and someone calls you out of the blue, you should hang up immediately, and they fail to do so.

Senator CARDIN. Let me just make one final point, and that is working with our State, in Maryland, our Comptroller has the ability to deal with paid preparers and is able to suspend their rights in Maryland. That, of course, has been compromised by the Supreme Court interpretation, and there will be an effort made to give the IRS the ability to regulate again those who are paid preparers.

Mr. Commissioner, I know you have supported that, and hopefully we can use that as an opportunity to work more closely with our States.

Commissioner KOSKINEN. Yes. We look forward to that. As I would say, the regulation is basically just requiring minimum standards in information, your ability to process tax returns. We are not talking about all sorts of other regulations.

So it really is appropriately described as requiring minimum standards of paid preparers.

Senator CARDIN. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator Casey?

Senator CASEY. Mr. Chairman, thank you very much. I want to thank the panel for being here and for your public service.

I am going to be addressing my question to Commissioner Koskinen. But I do want to say, because Mr. Dodaro has great Pennsylvania roots, that I apologize for probably not getting to you today, but I will tell everyone at Belle Vernon High School that you said hello. Is that okay?

Mr. DODARO. That is fine.

Senator CASEY. Thanks. And the chairman, of course, has Pennsylvania roots as well. So we want to highlight that.

I want to start with, Commissioner, some of the data points that you had in your testimony. I know I missed your presentation, but the written testimony highlights a number of things we should focus on in terms of the volume of your work.

In fiscal year 2015, you processed 244 million returns, issued more than $400 billion in refunds. Your new filters stopped 1.4 million returns filed by identity thieves, thereby preventing $8.7 billion in fraudulent returns.

So I wanted to state that for the record, because I know those numbers bear repeating. But I want to focus on two areas. One is cyber-criminals and the Security Summit, if you can comment on that, and also on tax scams.

With regard to the Security Summit itself, if you can just reiterate or amplify some of the earlier comments about some of the recommendations that came out of that Security Summit and, secondarily, how IRS can be more adaptive in terms of dealing with some of those security recommendations.

Commissioner KOSKINEN. What we all agreed on at our first meeting of the Security Summit—and we have been developing it since then—was that it would be critical to exchange information in real time. We are very sensitive about protecting taxpayer information and as a result, over the years, have not been particularly forthcoming with our partners about sharing information back.

One of their concerns was, they would give us leads and then we never told them whether the leads were good, and we never built on that.

So one of the purposes of the summit was to change all that and to have a robust exchange back and forth about patterns of activities, suspicious activities. We created a rapid response team with representatives from the States, the private sector, and the IRS. If there ever is a significant incident—and there have been a couple of them—we immediately have a way of getting that information out simultaneously.

They gave us and we all agreed on 20 different data points that we would get, what IP is being used on a computer, how long people are using it. If you are filing several returns very quickly, it is pretty clear you are not checking your deductions, you probably are a criminal filing.

So all of that has helped significantly. The additional funding we got from the Congress allows us to fund the development of the information center for analysis, which will simply facilitate more quickly the ability for States and the private sector to access the data rather than having it come in to us and then have us push it back out.

So we think that it is significant. It is important for it to be an ongoing partnership. One of the things that has been interesting to me was, at the first meeting, the private-sector preparers and software developers said that we, the IRS, are the only people who could set standards, and I told them that was fine as long as they worked with us to establish the standards as opposed to us just imposing them.

That is how we ended up with security standards; it is how we ended up with increased authentication standards that all the preparers are using this year.

We are working together to broaden those activities as we go forward. We will have more data points used in the next filing season, and we already see an up to 40 percent increase in the refund fraud stopped as a result of just sharing the information about leads.

Senator CASEY. Well, I appreciate that, and I hope as you begin to implement recommendations, that you keep us updated. Number two, if you find any either institutional obstacles or policy gaps that we can help with, I hope you tell us that.

I want to move, in the remaining seconds I have, to tax scams. I went across the State on our break and held a number of roundtables regarding senior scams more broadly, a lot of them having their origin in IRS impersonation or tax scams.

What can you tell us about that in terms of your recent work and what taxpayers should be focused on as we approach tax day?

Commissioner KOSKINEN. As we approach tax day, I think the most important thing for taxpayers to focus on is, if you are surprised to be hearing from us and you have not gotten a letter before—you should have gotten several letters—then you are not hearing from us. We never threaten people. We never tell you you are going to jail the next day, and we never tell you to make your payment to a bank account or a debit card.

If you are going to pay taxes, you pay them to the United States Treasury. If I could just get people—we have been working on this for over 2 years—to understand, (a) we do not threaten you; (b) we do not surprise you; and (c) if you are going to pay your taxes, make sure they go in a check payable to the United States Treasury.

TIGTA has been very good at working with us; the private-sector partnership has been good at working with us. They were the ones who said we have to have a public campaign to get taxpayers to pay attention to all of this.

Senator CASEY. Well, that "IRS will never do" list is something we read at various meetings, but we need to reemphasize that to give people the information so they understand that.

Commissioner KOSKINEN. The marketers say you have to make seven impressions before anybody hears you. We have tried to make more than seven impressions. TIGTA has been a wonderful partner with us with their work as well.

We have had very good coverage from the media, local and national media, over the last couple of years. But the people most vulnerable are elderly, are immigrants, low-income people who kind of live in a state of worry or fear, and they are the most likely to be prey to these kinds of events, which is why we are so concerned.

Senator CASEY. Thank you, Commissioner.

The CHAIRMAN. Senator Portman?

Senator PORTMAN. Thank you, Mr. Chairman. Thanks for holding this important hearing today. It is a topic that affects all of our constituents, I am sure.

I will tell you that in 2014, we had one case, one constituent case, of identity fraud. In 2015, we had 32. I do not know if that

is consistent across the States, but that kind of an increase, unfortunately, is an indication of the growing problem that we are all facing.

I am very concerned particularly about, Mr. George, your report, as the Inspector General for Tax Administration, indicating that the IRS has not established an IRS-wide approach to authenticating someone's identity.

I am open to more funding. I, for one, believe, as you know—we have talked about this—that more funding may be appropriate, as we did at year end, but I want to be sure the money is well spent. So I look forward to following up with you on that.

But I want to, if I could, shift to another issue this morning. It has to do, Commissioner Koskinen, with a very urgent issue for a group of our constituents. And Senator Brown and I have worked closely on this issue, and I think he has similar concerns to mine. I look forward to hearing from him on it in a moment.

But this has to do with the health coverage tax credit. As you know, section 407 of what is called the Trade Preferences Extension Act last year reinstated that health coverage tax credit through 2019. Basically, it extended the advance monthly payment program, which is essential. It is a program that gives advance premium payments to these HCTC recipients.

In that statute, the program was to be in place 1 year from the date of enactment. So in this case, we enacted it in June of 2015. We said that it would have to be in place by June 2016, this year, 1 year.

We were, unfortunately, told on March 7th of this year, 9 months after the bill had originally passed, by way of a letter from you, Mr. Commissioner, that the IRS would not be starting the advance monthly payment program by June, as required under law, but that you all hoped to start making advance payments by January of next year, so January of 2017.

So this has caused a huge problem. Six months go by, we do not hear anything, and then all of a sudden, taxpayers are told that the rug is being pulled out from under them and that we are not going to go ahead with this required advance payment program.

Expecting that they are going to get this advance monthly payment starting in mid-year, a lot of these taxpayers signed up for the health coverage in December and January. They thought they could get premium assistance, of course, starting on July 1st, as required under law.

This is not an easy decision to make. These premiums, as you know, are thousands of dollars per month. In some cases, taxpayers had to borrow money from family and friends, borrow from a bank, or take money from their retirement accounts early, to pay for these full premium prices in the first 6 months of this year, knowing that help was coming.

Furthermore, in some cases, these taxpayers had the option of receiving premium subsidies for plans on the health-care exchanges, but they turned down that opportunity because they wanted to stay in their private plans, which a lot of people do, and because they expected to get this 72.5-percent premium starting in July.

So, by the time the middle of March 2016 rolls around, these taxpayers have made a lot of life-altering decisions based on the fact that these advance payments are going to be there, and, again, they have the rug pulled out from under them.

These are resilient folks. They have been through a lot. These are people who were left behind, frankly, by our own Federal Government in terms of their health care and pensions. They can plan for stuff and they have done this.

When the HCTC was unavailable in 2014 and 2015, they made sacrifices and they got by, but, again, to pull a rug out from under them 3 months before they are expecting this help is unacceptable, completely unacceptable.

The fact that the IRS had July, August, September, October, November, and December of last year to provide them with some sort of notice, to me, is also unacceptable. And the option left to these taxpayers now of trying to find another way to fund these premiums for the next 6 months or to have to drop health-care plans altogether because they cannot afford them is also unacceptable.

So I understand our staffs—Senator Brown's staff and mine—have been working to try to find some sort of solution so that these advance monthly payment programs can get up and running by July. We have been having discussions about alternative methods of administering the advance monthly payment system so they are ready to go by July, as required by law.

I would just ask today, Mr. Commissioner, that, as you have in the past on some issues, you get personally involved in this and help us to work out an arrangement so that we can be sure that we do not have an unacceptable result.

Commissioner KOSKINEN. I have actually been personally involved since it was passed, because it is a critical program, and one of our obligations, we feel, is a high commitment to implement statutory mandates.

As we advised people when they were considering this, the last time the program was initiated, we got a $74-million appropriation to go with it, and that allowed us to hire a contractor to set the program up, and it ran well.

This time, we got no money, but we said, we are going to work to do our best. The reason we did not notify people until the 1st of March was, we worked very hard trying to see if, in addition to allowing people, which they can, to file in 2014 and 2015 for reimbursement, we could get the advance payment up and running, and as soon as we figured out that we would not be able to be up in June, we notified you and everyone else.

But I understand. Your points are well taken, and we do not take them lightly. If there were a way to do it, we would.

I would say in addition to the $74 million, the last time the program was set up, it took 2 years. If we can get it up and running by January—and we are committed to doing that—it will be a year and a half. So without any funding at all, we will be 6 months faster than the last time.

But your point is still valid. It does not necessarily help people who are, in fact, waiting for those payments. The fact that we will reimburse them after the fact is still a burden for them, and we regret that.

We are delighted to work with you and Senator Brown to find any way to get there before January, but we have to build systems to make payments. We normally do not make monthly payments. So we have no system to do it.

We can do the credit at the end of the year, because we give credits, which is why we could get 2014 and 2015 up and running. But we are delighted to work with you. We recognize that this is a burden on a number of people who have had a lot of other problems as well.

Senator PORTMAN. Well, it is a burden. Again, Mr. Chairman, thank you for your indulgence. But nothing you have said explains to me why we wait until March, mid-March of 2016, to tell people that these life-altering decisions that they made are not going to work out for them and they have to now find some alternative, which, in many cases, is going to mean, again, they are not going to have health-care coverage that they fully expected under law.

So I do hope that you will instead work with Senator Brown's staff and my staff to come up with an acceptable solution so that we can get these people some sort of coverage through this advance health-care payment.

Commissioner KOSKINEN. I would do that. The reason it took until February is, we actually made a good faith effort to see if we could get it done. We thought there was one possibility we could get it up and running. We worked on that and finally decided in February that the IT systems just would not be ready. But it was not because we did not care about it. It was because we were actually trying to see if we could make the one-year deadline. But we will work with you. We are delighted to do that.

The CHAIRMAN. Senator Nelson?

Senator NELSON. Thank you, Mr. Chairman.

Mr. Commissioner, you were kind enough to respond to my March letter on April 1st. I hope that it was not an April fool's joke. But here was one of the questions in the letter, and let me read to you your office's response to me, and I need a clarification.

The question was, under 26 CFR 1.501(c)(4)–1, the promotion of social welfare does not include direct or indirect participation or intervention in political campaigns on behalf or in opposition to any candidate for public office.

Given these requirements, please provide examples, Mr. Commissioner, of when it is permissible for 501(c)(4), 501(c)(5), or 501(c)(6) organizations to run ads supporting or attacking the positions of a candidate for elected office. Please provide examples of when this activity would be impermissible.

Now, I know this is a delicate subject, especially in front of the chairman and those of us over here. This was your answer, and I think it is quite clear, quote: "Unlike section 501(c)(3) charitable organizations, organizations described in section 501(c)(4), 501(c)(5), and 501(c)(6) are not prohibited from engaging in political campaign intervention. However, section 501(c) organizations that engage in political campaign intervention may be subject to tax under 527(f) on their exempt function expenditures. Whether an organization is engaged in political campaign intervention depends upon all the facts and circumstances of each case.

"Revenue ruling" such-and-such "2004–6 provides six examples illustrating facts and circumstances to be considered in determining whether a section 501(c) organization that engages in public policy advocacy has expended funds for a section 527 exempt function; that is, influencing or attempting to influence the selection, nomination, election, or appointment of any individual to public office."

The final couple of sentences read: "Revenue ruling 2007–41 provides an additional 21 examples illustrating facts and circumstances to be considered in determining whether a 501(c)(3) organization's activities result in political campaign intervention. The analysis reflected in these revenue rulings for determining whether an organization has engaged in political campaign intervention or has expended funds for a section 527 exempt function is fact-intensive. A copy of both revenue rulings is enclosed with this letter."

That was a very extensive answer, and I want you to know I appreciate it.

Now, here is the clarification that I need, please. So if that is the case, and if the IRS is really enforcing the law, how much tax revenue have you collected for political expenditures of 501(c)(4) groups this year or last year—or any year?

I fully do not expect you to have that on the top of your head, but I would like you to give the answer to this member of the committee.

Commissioner KOSKINEN. I carry around a lot of numbers in my head, but that is not one of them, as you suspected.

Senator NELSON. Understandably.

Commissioner KOSKINEN. Yes. We will be delighted to get you that information as quickly as we can, because it is important and we should be able to answer quickly.

Senator NELSON. That is great. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Nelson.

Senator Cantwell?

Senator CANTWELL. Thank you, Mr. Chairman. I thank the Senator for his work on this issue.

I wanted to ask of the Commissioner, one of the issues that I think all government faces is the shortage of highly skilled IT personnel, and we previously had support that would allow you to streamline the pay and authority so that you could get the skill level that you need.

My understanding is, though, that this legislative authority has expired and we need to re-legislate that streamlined authority so that you can have the critical pay.

So how much is this affecting us in getting the workers that we need at the IRS?

Commissioner KOSKINEN. Well, it is a significant challenge for us. We have only 13 or 14 people left. There were 40 slots. We never used more than 34 of that. There are 13 or 14 left; 10 are senior IT people working on cybersecurity, online services.

By this time next year, they will all be gone. Replacing them is very challenging for us at the IRS, although a lot of people want to come to us because we have very interesting challenges.

IT people, high-level people, are in great demand, and putting them through the hiring process—we find you, we like you, yet you

get to wait for 3 to 6 months while we put you through an application process. Our people are being recruited every day. Those people whom we are recruiting are being recruited every day.

So saying, "We really like you; we would like you to come work; sit still for 3 to 6 months, and we will get back to you," does not work. And so our concern is—and it is a serious concern—in the areas of information technology particularly, where we are talking about attracting the best in the country, without the authority—and we have not had it since 2013—it has made it almost impossible for us to recruit and retain at the level that we need to.

Senator CANTWELL. Is this affecting cybersecurity at the IRS?

Commissioner KOSKINEN. Our head of cybersecurity left recently rather than wait until his term ran out. The reason it is four plus two would allow us, for the people remaining, to have 2 years to, in fact, replace them as we go forward. But it is a critical need. It is not a major expenditure. It is not a lot of people. But it is critical to us, because it is focused on an area of high need for us.

Senator CANTWELL. Well, the competition for people knowledgeable in cybersecurity in general is very high, and IT still also remains very high.

So the fact is that, even in an "I can hire you tomorrow" environment, you are facing very, very stiff competition.

So I think, Mr. Chairman, this legislation—I think it keeps getting delayed or postponed based on markup, or maybe it is going to be on the next legislative schedule—it is really important for us to make sure that we have the flexibility.

I think the issue for all of our government is to continue to make sure that we have the best technology people, which is challenging for a whole lot of reasons. But I think that this authority to help you streamline that hiring and pay is something that we need to do as quickly as possible. So thank you.

Thank you, Mr. Chairman.

Commissioner KOSKINEN. Thank you, Senator.

The CHAIRMAN. I thank all of you for appearing here today. I also want to thank my colleagues for their participation.

Considering that tax day is just a few days away, I hope this hearing has helped us better understand the current environment for all taxpayers, and I hope to continue working with my colleagues from both sides of the aisle as we continue to examine ways to improve cybersecurity and better protect taxpayer information at the IRS.

I would ask that any questions for the record be submitted by Tuesday, April 26, 2016, and if you folks could get your answers back to us promptly, it would be very meaningful to us.

So with that, we will recess until further notice.

[Whereupon, at 11:54 a.m., the hearing was concluded.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

PREPARED STATEMENT OF HON. GENE L. DODARO, COMPTROLLER GENERAL OF THE UNITED STATES, GOVERNMENT ACCOUNTABILITY OFFICE

GAO–16–589T

April 12, 2016

INFORMATION SECURITY

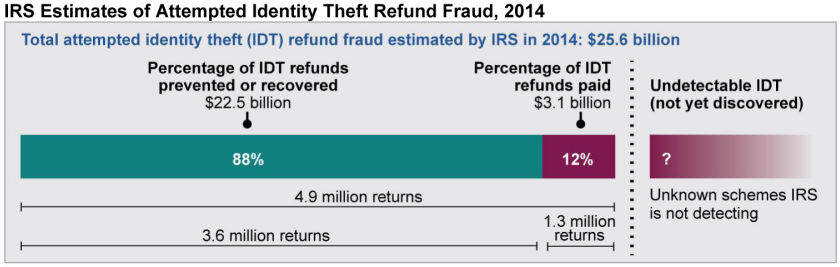
IRS Needs to Further Improve Controls Over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud

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 other controls intended to properly restrict access to systems and information, among other security measures. In particular, while IRS had improved some of its access controls, weaknesses remained in key controls for identifying and authenticating users, authorizing users' level of rights and privileges, encrypting sensitive data, auditing and monitoring network activity, and physically securing facilities housing its information technology resources. These weaknesses were due in part to IRS's inconsistent implementation of its agency-wide security program, including not fully implementing prior GAO recommendations. GAO concluded that these weaknesses collectively constituted a significant deficiency for the purposes of financial reporting for fiscal year 2015. As a result, taxpayer and financial data continue to be exposed to unnecessary risk.

Identity theft refund fraud also poses a significant challenge. IRS estimates it paid $3.1 billion in these fraudulent refunds in filing season 2014, while preventing $22.5 billion (see figure). The full extent is unknown because of the challenges inherent in detecting this form of fraud.

IRS Estimates of Attempted Identity Theft Refund Fraud, 2014



Source: GAO analysis of IRS data. | GAO-16-589T

IRS has taken steps to combat identity theft refund fraud such as improving phone service for taxpayers to report suspected identity theft and working with industry, States, and financial institutions to detect and prevent it. However, as GAO reported in August 2014 and January 2015, additional actions can further assist the

agency in addressing this crime, including pre-refund matching of taxpayer returns with information returns from employers, and assessing the costs, benefits, and risks of improving methods for authenticating taxpayers. In addition, the Consolidated Appropriations Act 2016 includes a provision that would help IRS with pre-refund matching and also includes an additional $290 million to enhance cybersecurity, combat identity theft refund fraud, and improve customer service.

According to IRS and industry partners, the 2016 filing season has generally gone smoothly, with about 95 million returns and $215 billion in refunds processed through April 1, 2016. In addition, IRS increased its level of phone service to taxpayers, although it has not developed a comprehensive strategy for customer service as GAO recommended in December 2015.

Chairman Hatch, Ranking Member Wyden, and members of the committee:

Thank you for the opportunity to testify on cybersecurity and protecting taxpayer information. As taxpayers file their returns for 2015, it is especially important that the Internal Revenue Service (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. Recent information security incidents at IRS further highlight the importance of ensuring that these controls are effectively implemented.

As you know, the filing season is the time when most taxpayers interact with IRS. As in previous years, a major challenge during the filing season is protecting taxpayers' information and addressing identity theft (IDT) refund fraud, which 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.[3] This crime burdens honest taxpayers because authenticating their identities is likely to delay processing their 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 the enforcement of our tax laws high-risk area to include IRS's efforts to address IDT refund fraud.[4]

My statement today focuses on opportunities to assist IRS in addressing (1) information security weaknesses we have identified and (2) the challenge of identity theft refund fraud. I will also discuss the status of selected IRS filing season operations.

Within the context of my testimony, it is important to note that, for fiscal year 2016, IRS received about $290 million in additional funding to support these areas. Specifically, the funding was intended to improve customer service, IDT identification and prevention, and cybersecurity efforts.[5] According to IRS's spending plan this funding will be used to invest in (1) increased telephone level of service, including reduced wait times and improved performance on IRS's Taxpayer Protection Program/Identity Theft Toll Free Line ($178.4 million); (2) cybersecurity including

---

[1] PII 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.

[2] *See* GAO, *High-Risk Series: An Update,* GAO–15–290 (Washington, DC: Feb. 11, 2015).

[3] This statement discusses IDT refund fraud and not employment fraud. IDT employment fraud occurs when an identity thief uses a taxpayer's name and Social Security number to obtain a job.

[4] GAO–15–290.

[5] Consolidated Appropriations Act, 2016, Pub. L. No. 114–113, div. E, § 113, 129 Stat. 2242 (Dec. 18, 2015).

network security improvements, protection from unauthorized access, and enhanced insider threat detection ($95.4 million); and (3) IDT refund fraud prevention ($16.1 million).

My statement is based in part on our previous reports issued between August 2014 and March 2016. We updated selected data in this statement with 2016 data from IRS on individual income tax return processing and telephone service, as well as IRS's fiscal year 2016 spending plan for the additional $290 million in appropriated funds. We also incorporated IRS statements on recent data breaches and IRS actions to address our past recommendations. To assess data reliability, we reviewed IRS data and documentation and assessed documentation for data limitations. We found the data to be sufficiently reliable for our purposes. 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

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. 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, DC, headquarters and at more than 550 offices in all 50 States, U.S. territories, and some U.S. embassies and consulates. Each filing season IRS provides assistance to tens of millions of taxpayers over the phone, through written correspondence, online, and face-to-face. The scale of these operations alone presents challenges.

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. Accordingly, it is critical for IRS to effectively implement information security controls and an agency-wide information security program in accordance with Federal law and guidance.[6]

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.[7] 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, IRS reported this number to be about 114,000, and 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 of identity theft (IDT) to help prevent future IDT refund fraud.[8] The service on IRS's website allowed taxpayers to re-

[6] In particular, the Federal Information Security Modernization Act of 2014 (FISMA), 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. Pub. L. No. 113–283, § 2(a), 128 Stat. 3074 (Dec. 18, 2014), codified at 44 U.S.C. § 3554(a).

[7] This 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.

[8] In 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 re-

Continued

trieve 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 before resuming service. As of April 7, the online service was still suspended.

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.

ALTHOUGH IRS HAS MADE IMPROVEMENTS, INFORMATION SECURITY WEAKNESSES CONTINUE TO PLACE TAXPAYER AND FINANCIAL DATA AT RISK

As we reported in March 2016,[9] IRS has implemented numerous controls over key financial and tax processing systems; however, it had not always effectively implemented access and other controls,[10] including elements of its information security program.

Access controls are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. These controls include identification and authentication, authorization, cryptography, audit and monitoring, and physical security controls, among others. In our most recent review we found 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 multifactor authentication [11] 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.
- **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 it 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.
- **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

---

ceive an IP PIN. IP PINs help prevent future IDT refund fraud 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. *See* GAO, *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud,* GAO–14–633 (Washington, DC: Aug. 20, 2014), for more details on IRS's IP PIN service.

[9] GAO, *Information Security: IRS Needs to Further Improve Controls Over Financial and Taxpayer Data,* GAO–16–398 (Washington, DC: Mar. 28, 2016).

[10] Information security controls include logical and physical access controls, configuration management, and continuity of operations. These controls are designed to ensure that access to data is properly restricted, physical access to sensitive computing resources and facilities is protected, systems are securely configured to avoid exposure to known vulnerabilities, and backup and recovery plans are adequate and tested to ensure the continuity of essential operations.

[11] 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).

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 information technology (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 2 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 addressed previously identified deficiencies or ensured that its corrective actions were effective. During our most recent review, IRS told us it had addressed 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.[12]

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 rec-

[12] A 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.

ommendations in a separate report with limited distribution to address 26 new weaknesses in access controls and configuration management.[13]

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 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–16–589T

In commenting on drafts of our 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.

In addition, IRS can take steps to improve its response to data breaches. 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 the Office of Management and Budget and the National Institute of Standards and Technology.[14] 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

[13] GAO, *Information Security: IRS Needs to Further Improve Controls Over Financial and Taxpayer Data,* GAO–16–397SU (Washington, DC: Mar. 28, 2016).

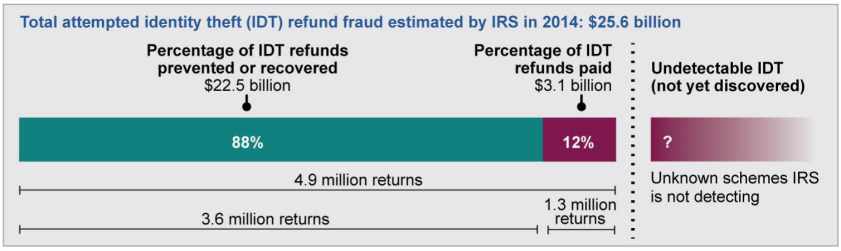
[14] GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent,* GAO–14–34 (Washington, DC: Dec. 9, 2013).

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.

BILLIONS OF DOLLARS HAVE BEEN LOST TO IDT REFUND FRAUD, AND IRS FACES CHALLENGES IN COMBATING THIS EVOLVING THREAT

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. 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 (see figure 1).[15] However, IRS also estimated, where data were available, that it paid $3.1 billion in fraudulent IDT refunds. Because of the difficulties in knowing the amount of undetectable fraud, the actual amount could differ from these estimates.

Figure 1: IRS Estimates of Attempted Identity Theft Refund Fraud, 2014



Source: GAO analysis of IRS data. | GAO-16-589T

IRS has taken steps to address IDT refund fraud; however, it remains a persistent and continually changing threat. IRS recognized the challenge of IDT refund fraud in its fiscal year 2014–2017 strategic plan and increased resources dedicated to combating IDT and other types of refund fraud.[16] In fiscal year 2015, IRS reported that it staffed more than 4,000 full-time equivalents and spent about $470 million on all refund fraud and IDT activities.[17] As described above, IRS received an additional $290 million for fiscal year 2016 to improve customer service, IDT identification and prevention, and cybersecurity efforts and the agency plans to use $16.1 million of this funding to help prevent IDT refund fraud, among other things. The administration requested an additional $90 million and an additional 491 full-time equivalents for fiscal year 2017 to help prevent IDT refund fraud and reduce other improper payments.[18] IRS estimates that this $90 million investment in IDT refund fraud and other improper payment prevention would help it protect $612 million in revenue in fiscal year 2017, as well as protect revenue in future years.

IRS has taken action to improve customer service related to IDT refund fraud. For example, between the 2011 and 2015 filing seasons, IRS experienced a 430 percent increase in the number of telephone calls to its Identity Theft Toll Free Line—

[15] IRS's 2014 estimates cannot be compared to 2013 estimates because of substantial methodology changes to better reflect new IDT refund fraud schemes and to improve the accuracy of its estimates, according to IRS officials. GAO is reviewing IRS's IDT refund fraud estimates as part of ongoing work.

[16] IRS, *Strategic Plan:* FY 2014–2017, (Washington, DC: June 2014).

[17] IRS officials told us they do not track spending for identity theft activities separately from other types of refund fraud. A full-time equivalent reflects the total number of regular straight-time hours (*i.e.,* not including overtime or holiday hours) worked by employees divided by the number of compensable hours applicable to each fiscal year.

[18] Improper payments are payments that should not have been made or that were made in an incorrect amount (including overpayments and underpayments).

as of March 19, 2016, IRS had received over 1.1 million calls to this line.[19] Moreover, 77 percent of callers seeking assistance on this telephone line received it compared to 54 percent during the same period last year. Average wait times during the same period have also decreased—taxpayers are waiting an average of 14 minutes to talk to an assistor, a decrease from 27 minutes last year.

IRS also works with third parties, such as tax preparation industry participants, States, and financial institutions to try to detect and prevent IDT refund fraud. In March 2015, the IRS Commissioner convened a Security Summit with industry and States to improve information sharing and authentication. IRS officials said that 40 State departments of revenue and 20 tax industry participants have officially signed a partnership agreement to enact recommendations developed and agreed to by summit participants. IRS plans to invest a portion of the $16.1 million it received in fiscal year 2016 into identity theft prevention and refund fraud mitigation actions from the Security Summit. These efforts include developing an Information Sharing and Analysis Center where IRS, States, and industry can share information to combat IDT refund fraud.

Even though IRS has prioritized combating IDT refund fraud, fraudsters adapt their schemes to identify weaknesses in IDT defenses, such as gaining access to taxpayers' tax return transcripts through IRS's online Get Transcript service.[20] According to IRS officials, with access to tax transcripts, fraudsters can create historically consistent returns that are hard to distinguish from a return filed by a legitimate taxpayer, potentially making it more difficult for IRS to identify and detect IDT refund fraud.

Implementing Past GAO Recommendations Could Help IRS Combat IDT Refund Fraud

Without additional action by IRS and Congress, the risk of issuing fraudulent IDT refunds could grow. We previously made recommendations to IRS to help it better combat IDT refund fraud:

- **Authentication.** In January 2015, we reported that IRS's authentication tools have limitations and recommended that IRS assess the costs, benefits and risks of its authentication tools.[21] For example, individuals can 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, according to our analysis and interviews with tax software and return preparer associations and companies. After filing an IDT return using an e-file PIN, the fraudulent return would proceed through IRS's normal return processing.

  In November 2015, IRS officials told us that the agency had developed guidance for its Identity Assurance Office to assess costs, benefits, and risk, and that its analysis will inform decision-making on authentication-related issues. IRS also noted that the methods of analysis for the authentication tools will vary depending on the different costs and other factors for authenticating taxpayers in different channels, such as online, phone, or in-person. In February 2016, IRS officials told us that the Identity Assurance Office plans to complete a strategic plan for taxpayer authentication across the agency in September 2016. While IRS is taking steps, it will still be vulnerable until it completes and uses the results of its analysis of costs, benefits, and risk to inform decision-making.

- **Form W–2, Wage and Tax Statement (W–2) Pre-refund Matching.** In August 2014 we reported that the wage information that employers report on Form W–2 is not available to IRS until after it issues most refunds, and that if IRS had access to W–2 data earlier, it could match such information to taxpayers' returns and identify discrepancies before issuing billions of dollars of fraudulent IDT refunds.[22] We recommended that IRS assess the costs and benefits of accelerating W–2 deadlines.

---

[19] Total call volume to IRS's identity theft protection toll free telephone line includes automated and assistor calls answered, as well as those that received a busy signal or were abandoned or disconnected.

[20] As mentioned above, the online Get Transcript service has been unavailable since May 2015.

[21] GAO, *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, DC: Jan. 20, 2015).

[22] GAO, *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud,* GAO–14–633 (Washington, DC: Aug. 20, 2014).

In response to our recommendation, IRS provided us with a report in September 2015 discussing (1) adjustments to IRS systems and work processes needed to use accelerated W–2 information, (2) the potential impacts on internal and external stakeholders, and (3) other changes needed to match W–2 data to tax returns prior to issuing refunds, such as delaying refunds until W–2 data are available. In December 2015, the Consolidated Appropriations Act of 2016 amended the tax code to accelerate W–2 filing deadlines to January 31.[23] IRS's report will help IRS determine how to best implement pre-refund W–2 matching, given the new January 31st deadline for filing W–2s. Additionally, we suggested that Congress should consider providing the Secretary of the Treasury with the regulatory authority to lower the threshold for electronic filing of W–2s, which could make more W–2 information available to IRS earlier.

- **External Leads.** IRS partners with financial institutions and other external parties to obtain information about emerging IDT refund trends and fraudulent returns that have passed through IRS detection systems. In August 2014, we reported that IRS provides limited feedback to external parties on IDT external leads they submit and offers external parties limited general information on IDT refund fraud trends and recommended that IRS provide actionable feedback to all lead generating third parties.[24]

  In November 2015, IRS reported that it had developed a database to track leads submitted by financial institutions and the results of those leads. IRS also stated that it had held two sessions with financial institutions to provide feedback on external leads provided to IRS. In December 2015, IRS officials stated that the agency sent a customer satisfaction survey asking financial institutions for feedback on the external leads process and was considering other ways to provide feedback to financial institutions. In April 2016, IRS officials stated they plan to analyze preliminary survey results by mid-April 2016. Additionally, IRS officials reported that the agency shared information with financial institutions in March 2016 and plans to do so on a quarterly basis, with the next information sharing session scheduled in June 2016.

THE 2016 FILING SEASON HAS GENERALLY BEEN SMOOTH, AND TELEPHONE SERVICE HAS IMPROVED

IRS and industry partners have characterized that returns processing and refund issuance during this filing season has been generally smooth. Through April 1, 2016, IRS had processed about 95 million returns and issued 76 million refunds totaling about $215 billion. While IRS experienced a major system failure in February that halted returns processing for about a day, the agency reported that it had minimal effect on overall processing of returns and refunds.

In addition to filing returns, many taxpayers often call IRS for assistance. IRS's telephone service has generally improved in 2016 over last year. From January 1 through March 19, 2016 IRS received about 35.4 million calls to its automated and live assistor telephone lines, about a 2 percent decrease compared to the same period last year.[25] Of the 13.4 million calls seeking live assistance, IRS had answered 9.1 million calls—a 75 percent increase over the 5.2 million calls answered during the same period last year.

IRS anticipated that 65 percent of callers seeking live assistance would receive it this filing season, which runs through April 18, and 47 percent of callers would receive live assistance through the entire 2016 fiscal year.[26] As of March 19, 2016, 75 percent of callers had received live assistance, an increase from 38 percent during the same period last year. Further, the average wait time to speak to an assistor also decreased from 24 to 9 minutes. As we reported in March 2016, however, IRS's telephone level of service for the full fiscal year has yet to reach the levels it had achieved in earlier years.[27]

---

[23] Pub. L. No. 114–113, div. Q, § 201, 129 Stat. 2242 (Dec. 18, 2015). This change goes into effect for W–2s reporting payments made in 2016 and filed in 2017.

[24] GAO–14–633.

[25] Total call volume to IRS's toll free telephone lines include automated and assistor calls answered, as well as those that received a busy signal or were abandoned or disconnected.

[26] This year, most taxpayers have until April 18 to file a tax return with IRS. IRS's projected telephone level of service for the filing season covers the period between January 1, 2016 and April 23, 2016.

[27] GAO, *Internal Revenue Service: Preliminary Observations on the Fiscal Year 2017 Budget Request and 2016 Filing Season Performance,* GAO–16–459R (Washington, DC: Mar. 8, 2016).

IRS attributed this year's service improvement to a number of factors. Of the additional $290 million IRS received in December 2015, it allocated $178.4 million (61.5 percent) for taxpayer services to make measurable improvements in its telephone level of service. With the funds, IRS hired 1,000 assistors who began answering taxpayer calls in March, in addition to the approximately 2,000 seasonal assistors it had hired in fall 2015.[28] To help answer taxpayer calls before March, IRS officials told us that they detailed 275 staff from one of its compliance functions to answer telephone calls.[29] IRS officials said they believe this step was necessary because the additional funding came too late in the year to hire and train assistors to fully cover the filing season. IRS also plans to use about 600 full-time equivalents of overtime for assistors to answer telephone calls and respond to correspondence in fiscal year 2016, compared to fewer than 60 full-time equivalents of overtime used in fiscal year 2015.

In December 2014, we recommended that IRS systematically and periodically compare its telephone service to the best in business to identify gaps between actual and desired performance.[30] IRS disagreed with this recommendation, noting that it is difficult to identify comparable organizations. We do not agree with IRS's position; many organizations run call centers that would provide ample opportunities to benchmark IRS's performance.

In fall 2015, Department of the Treasury (Treasury) and IRS officials said they had no plans to develop a comprehensive customer service strategy or specific goals for telephone service tied to the best in the business and customer expectations. Without such a strategy, Treasury and IRS can neither measure nor effectively communicate to Congress the types and levels of customer service taxpayers should expect and the resources needed to reach those levels. Therefore, in December 2015 we suggested that Congress consider requiring that Treasury work with IRS to develop a comprehensive customer service strategy.[31] In April 2016, IRS officials told us that the agency established a team to consider our prior work in developing this strategy or benchmarking its telephone service.

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 and the public are 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.

Weaknesses in information security can also increase the risk posed by identity theft refund fraud. IRS needs to establish an approach for addressing identity theft refund fraud that is informed by assessing the cost, benefits, and risks of IRS's various authentication options and improving the reliability of fraud estimates.

While this year's tax filing season has generally gone smoothly and IRS has improved customer service, it still needs to develop a comprehensive approach to customer service that will meet the needs of taxpayers while ensuring that their sensitive information is adequately protected.

Chairman Hatch, Ranking Member Wyden, and members of the committee, this concludes my statement. I look forward to answering any questions that you may have at this time.

---

[28] In contrast, IRS reduced the number of assistors answering telephone calls between fiscal years 2010 and 2015, which contributed to the lowest level of telephone service in fiscal year 2015 compared to recent years.

[29] IRS has not yet determined the amount of foregone revenue from taking this action.

[30] GAO, *Tax Filing Season: 2014 Performance Highlights the Need to Better Manage Taxpayer Service and Future Risks,* GAO–15–163 (Washington, DC: Dec. 16, 2014).

[31] GAO, *2015 Tax Filing Season: Deteriorating Taxpayer Service Underscores Need for a Comprehensive Strategy and Process Efficiencies,* GAO–16–151 (Washington, DC: Dec. 16, 2015).

PREPARED STATEMENT OF HON. J. RUSSELL GEORGE, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, DEPARTMENT OF THE TREASURY

Chairman Hatch, Ranking Member Wyden, and members of the committee, thank you for the opportunity to testify on the Internal Revenue Service's (IRS) controls to protect sensitive taxpayer information.

The Treasury Inspector General for Tax Administration (TIGTA) is statutorily mandated to provide independent audit and investigative services necessary to improve the economy, efficiency, and effectiveness of IRS operations, including the IRS Chief Counsel. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA's role is critical in that we provide the American taxpayer with assurance that the approximately 86,000 IRS employees [1] who collected over $3.3 trillion in tax revenue, processed over 244 million tax returns, and issued more than $400 billion in tax refunds during Fiscal Year (FY) [2] 2015,[3] 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 IRSemployees 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 more than 670 IRS facilities nationwide.

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. 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 reported that more than 1,000 security incidents occurred to its systems during the period August 1, 2014, to July 31, 2015.

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 Identi-

[1] Total IRS staffing as of October 3, 2015. Included in the total are approximately 15,400 seasonal and part-time employees.
[2] The Federal Government's fiscal year begins on October 1 and ends on September 30.
[3] IRS, *Management's Discussion and Analysis, Fiscal Year 2015.*
[4] Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act* (Mar. 2016).

fiable Information. For Calendar Year 2015, the IRS processed more than 150 million individual tax returns and 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 ability to prevent and detect breaches to its computer systems and the IRS's processes to authenticate users accessing its online services.

DATA SECURITY REMAINS A TOP CONCERN OF TIGTA

Since FY 2011, 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. To provide oversight of the IRS's Information Security program, TIGTA conducts ongoing audit coverage of various security programs, systems, and solutions. As of March 2016, 14 TIGTA audits still have 23 recommendations that have yet to be implemented. These recommendations address weaknesses related to connections with external partners, continuous efforts to monitor information security, implementation of the Homeland Security Presidential Directive 12 initiative,[5] and information technology asset management.

TIGTA continues to identify significant security weaknesses that could affect the confidentiality, integrity, and availability of financial and sensitive taxpayer data. For example, during our most recent Federal Information Security Modernization Act[6] evaluation of the IRS's information security programs and practices,[7] 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 performance specified by the Department of Homeland Security.[8]

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.

Specifically, we reported that the IRS Continuous Monitoring Management program is at a maturity level of one on a scale of one to five, where one is the least mature and five is the most mature. In July 2014, the Department of the Treasury decided to adopt a uniform approach across the Department and to use the toolset selected by the Department of Homeland Security to meet the program requirements. The Department of Homeland Security is currently in the process of procuring a standard set of cybersecurity tools and services for use by Federal agencies. These tools will include sensors that perform automated searches for known cyber flaws and send the results to dashboards that inform system managers in real time of cyber risks that need remediation.

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. Home-

[5] Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal identity credentials to ensure that only authorized personnel have access to Government systems and applications.

[6] 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.

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

[8] 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.

land 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. Specifically, these processes have not been fully implemented enterprise-wide and still rely on many tedious manual procedures. Eventually, the IRS's Configuration Management program will benefit from the implementation of the Information Security Continuous Monitoring program, which is intended to automate configuration management in real time for the universe of IRS assets.

Patch [9] management is an important element in mitigating the security risks associated with known vulnerabilities to computer systems. This is critical to prevent intrusions by unauthorized individuals or entities. TIGTA evaluated the effectiveness of the IRS security patch management process, which has been an ongoing challenge for the IRS.[10] In 2012, we found that the IRS had made progress in automating installation and monitoring in a large segment of its computers, but it had not yet implemented key patch management policies and procedures needed to ensure that all IRS systems are patched timely and operating securely. Any significant delays in patching software with critical vulnerabilities provides ample opportunity for persistent attackers to gain control of vulnerable computers and get access to the sensitive data the computer systems may contain, including taxpayer data. The Government Accountability Office reported in March 2015 that the IRS was still not effectively applying security patches in a timely manner.[11] We also reported in September 2015 that the IRS is still working to expand a standard automated process to deploy operating system patches enterprise-wide.[12]

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 identified areas for improvement.[13] 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. 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.[14]

TIGTA also found that many interconnections [15] 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 inter-

[9] A patch fixes a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.

[10] TIGTA, Ref. No. 2012–20–112, *An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers* (Sept. 2012).

[11] GAO–15–337, *IRS Needs to Continue Improving Controls over Financial and Taxpayer Data* (Mar. 2016).

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

[13] 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).

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

[15] 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.

connections that are active but lack proper approvals and assurances necessary to meet current security requirements.[16]

In addition, TIGTA reported[17] that the IRS was unable to upgrade all of its workstations with the most current Windows® operating system.[18] 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 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.

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 plans to increase the availability and quality of self-service interactions, allowing it to free up in-person resources for taxpayers who truly need them. 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. As tax administration evolves, the challenge of providing adequate data security will continue.

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.[19] As a result, the level of authentication the IRS uses for its various services is not consistent. 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 development and integration of all forms of authentication, including frameworks, policies, and processes across the IRS.

Office of Management and Budget (OMB) Memorandum M–04–04, *E-Authentication for Federal Agencies,*[20] 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.

---

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

[17] TIGTA, Ref. No. 2015–20–073, *Inadequate Early Oversight Led to Windows Upgrade Project Delays* (Sept. 2015).

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

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

[20] OMB, M–04–04, *E-Authentication for Federal Agencies* (Dec. 2003).

In addition, the U.S. Department of Commerce National Institute of Standards and Technology (NIST) *Special Publication 800–63–2, Electronic Authentication Guideline*[21] provides the technical requirements for the four levels of assurance defined in OMB guidance as shown in the following table.

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)[22] applications found that these authentication methods provide only single-factor authentication despite NIST standards requiring multifactor authentication for such high-risk applications.

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.

The IRS's current e-Authentication framework also 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

[21] NIST, NIST SP–800–63–2, *Electronic Authentication Guideline* (Aug. 2013).

[22] 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).

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.

In August 2015, the IRS indicated that unauthorized users had been successful[23] in obtaining tax information[24] on the Get Transcript application for an estimated 334,000 taxpayer accounts. 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.

TIGTA's current review[25] 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 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.[26] To date, we have learned that the IRS is working with the U.S. Digital Service[27] on its new e-authentication and authorization policies and procedures. In addition, TIGTA is participating in a multiagency 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 reac-

---

[23] 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.

[24] The tax information that can be accessed on the Get Transcript application can include the current and 3 prior years of tax returns, 9 years of tax account information, and wage and income information.

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

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

[27] 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.

tivated 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.

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.

On February 9, 2016, the IRS announced that it had identified and halted an automated botnet[28] attack on its Electronic Filing (e-file) PIN application on *IRS.gov*. Using personal data stolen elsewhere outside the IRS, identity thieves used malware in an attempt to generate e-file PINs for stolen Social Security Numbers (SSN). An e-file PIN is used in some instances to electronically file a tax return. While no personal taxpayer data was compromised or disclosed by IRS systems in the attack, the IRS did identify unauthorized attempts involving approximately 464,000 unique SSNs, of which 101,000 were used to successfully access an e-file PIN.

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.

In response to concerns expressed by the IRS Commissioner during 2015, the IRS received an additional $290 million in appropriated funds for FY 2016. The IRS plans to use $111.5 million of the additional funding to enhance cybersecurity to safeguard taxpayer data. Specifically, the IRS plans to increase staffing, replace outdated equipment, and make network improvements for monitoring and analyzing data traffic. In addition, the IRS plans to implement actions from the Security Summit[29] and to relaunch the Get Transcript application. We are planning a review to assess IRS's use of these funds to improve cybersecurity.

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.

Chairman Hatch, Ranking Member Wyden, and members of the committee, thank you for the opportunity to share my views.

PREPARED STATEMENT OF HON. ORRIN G. HATCH,
A U.S. SENATOR FROM UTAH

WASHINGTON—Senate Finance Committee Chairman Orrin Hatch (R–Utah) today delivered the following opening statement at a hearing examining how the Internal Revenue Service (IRS) is safeguarding private taxpayer information this filing season and to determine what improvements may be necessary for the agency to fully protect taxpayers from cybercriminals:

---

[28] A botnet is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or malware) to other computers on the Internet, usually for the purpose of a cyberattack or denial of service attack.

[29] On March 19, 2015, the IRS Commissioner convened a meeting with IRS officials, the chief executive officers of the leading tax preparation firms, software developers, payroll and tax financial product processors, and representatives from 22 States to discuss common challenges and ways to leverage their collective resources and efforts for identity theft detection and prevention.

Good morning. It's a pleasure to welcome everyone to today's hearing, which we've titled "Cybersecurity and Protecting Taxpayer Information."

These are important issues that the Finance Committee has been working on for some time. In June of last year, for example, we held a hearing on the theft of Internal Revenue Service data affecting taxpayer information. Much has happened since that time.

At the urging of the Finance Committee, the IRS, State revenue commissioners, and leaders in the tax return preparation industry came together last year to convene a Security Summit, which resulted in new information-sharing agreements to help identify suspicious activity in the tax filing and refund process. We look forward to hearing more about that effort today.

But in the face of this progress, we have also seen unprecedented growth in the scope and scale of cyber-attacks aimed at stealing personal information and billions of dollars from taxpayers.

Last year alone, cyber-criminals obtained access to sensitive personal information from several large health insurers, exposing tens of millions of Americans to potential identity theft. Foreign governments gained access to poorly protected Federal Government databases, including a treasure trove of information at the Office of Personnel Management.

Today we will focus on three separate aspects of this problem.

First, we will consider the ways the IRS authenticates taxpayer identities to prevent data thieves from using authentication information to gain access to even more information about taxpayers or to file false returns and obtain refunds under stolen identities.

Second, we will examine how the IRS uses its resources to improve cybersecurity. This will include some discussion about the IRS Future State plan, which the agency has developed in order to adapt to the realities of the 21st century.

Third and finally, we will consider the ongoing joint efforts of the IRS, State revenue collectors, and private tax preparers to see what can be accomplished to better secure taxpayer information and protect taxpayers from fraud.

Taking a look at our witness table, it is clear that this is not a typical lineup of witnesses. Challenges to cyber-security require not only smart and persistent leadership up at the top, but also technological expertise and up-to-date skills down on the ground. So today, we not only have with us the heads of the IRS, the Government Accountability Office, and the Treasury Inspector General for Tax Administration, we've invited subject matter experts on the relevant issues from each of those agencies to testify as well.

That's a total of six witnesses. And, I suspect each of them will bring unique and important insights to this discussion.

In closing, I'll just say that, while we are clearly making real progress in this area, the challenges are continuing to grow and criminals behind this kind of data theft are getting more sophisticated and aggressive, seemingly by the day. And, American taxpayers—and their livelihoods—are their targets.

In other words, we have a lot of work to do. My hope is that we'll continue to be able to work on these issues on a bipartisan basis in order to do right by the American people.

PREPARED STATEMENT OF HON. JOHN KOSKINEN, COMMISSIONER, INTERNAL REVENUE SERVICE

INTRODUCTION

Chairman Hatch, Ranking Member Wyden, and members of the committee, 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 1 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 ofgovernment 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 e-mail 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 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, crimi-

nals 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 toundergo 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 9-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 e-mail 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, DC—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 Transcriptonline 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 $16.1 million 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.

Chairman Hatch, Ranking Member Wyden, and members of the committee, this concludes my statement. I would be happy to take your questions.

PREPARED STATEMENT OF HON. RON WYDEN,
A U.S. SENATOR FROM OREGON

Hackers and crooks, including many working for foreign crime syndicates, are jumping at every opportunity they have to steal hard-earned money and sensitive personal data from U.S. taxpayers. It happens online and in the real world. And in my view, taxpayers have been failed by the agencies, the companies, and the policymakers here in Congress they rely on to protect them.

It was unacceptable for the IRS to leave the front door open to hackers by using a weak authentication process for its Get Transcript system. It meant thieves could walk through the door and steal the tax information of three quarters of a million taxpayers.

And to make matters worse, after the IRS mailed special Identity Protection PIN numbers to the hacking victims, it repeated its mistake and used lax security online. For the tax scammers, once again it was as easy as going online, plugging in the personal data you've already stolen, and pretending to be somebody who's lost their IP PIN. So after leaving the front door open, the IRS left the back door open, too. There is no excuse for this.

But poor protection of taxpayer information is not just a problem at the IRS—there's a lot of blame to go around. Already this tax season, hackers have gotten into the inadequately guarded systems of private software firms and stolen personal information from thousands of people. And it's my judgement that you can't have an honest discussion about protecting taxpayer information without including the vulnerabilities from e-file providers, as well as crooked return preparers who operate in the shadows and steal from customers.

For years Republicans and Democrats agreed on the need for minimum standards for return preparers, but Congress has sat back and watched while criminals have come in and preyed on taxpayers. When it comes to blocking hackers, Congress has done next to nothing while the IRS loses its ability to hire the experts who can keep taxpayer information safe.

If you're a top-notch tech expert, you're already taking a pay cut to work in public service compared to what you'd earn at firms in Oregon or California. Now, without what's called "streamlined critical pay authority," it can take 4 to 6 months to bring a new hire on board at the IRS. So let's be clear: taxpayer information is under assault every day, but the IRS does not have the legal authority it needs from Congress to build a cybersecurity team that can beat back the crooks.

Already there's been an exodus of high-ranking IRS tech staff. The Director of Cybersecurity Operations left a month ago. The terms for the remaining employees working under this authority continue to expire, including for one of our witnesses, Chief Technology Officer Terence Milholland. Come 2017, there will not be any left.

So today, instead of rehashing the past and beating up on one agency or one firm, this committee ought to focus on how to step up the fight against hackers and crooks across the board. It's my view that streamlined critical pay authority is a key part of the solution. There was a bipartisan bill ready to go last fall, and this committee ought to move forward on it as soon as possible. Furthermore, Congress needs to make more than token investments in IT at the IRS. Congress has held the IRS' tech budget below where it was 6 years ago, but you can bet that the hackers haven't backed down since then.

Next, the IRS and private firms need to do much more to keep taxpayer information safe in their systems. The Get Transcript hack I mentioned earlier has been well documented. And a recent audit by the Online Trust Alliance found that the security maintained by private free-file services did not meet expectations. It is unacceptable for troves of taxpayer data to be more vulnerable to hacking than many social media or e-mail accounts. And the committee ought to consider whether the

IRS has the authority it needs to guarantee that the security used by private software firms is up to snuff.

While many tax preparers are honest practitioners, there are always some bad apples in the barrel. Last year Senator Cardin and I introduced a bill giving IRS the authority to regulate tax return preparers. Senator Hatch and I have worked to create a bipartisan identity theft bill for markup in the Finance Committee, which I had hoped would include the regulation of return preparers. It is still my view that people handling sensitive taxpayer information should meet minimum standards and that the committee should vote to require that.

It's already open season for hackers to steal money and data from hard-working Americans, so congressional inaction should not make the situation worse. With tax day approaching, millions of Americans are filing their returns online, through the mail, or with a private return preparer. This committee has a responsibility to protect taxpayers no matter what filing method they choose. So I see this hearing as an opportunity to find bipartisan solutions on all fronts.

COMMUNICATION

STATEMENT FOR THE RECORD BY KWAME GYAMFI

"Cybersecurity and Protecting Taxpayer Information"

April 12, 2016

Senate Committee on Finance
Dirksen Senate Office Building
Washington, DC 20510–6200

I had the opportunity to attend the "Cybersecurity and Protecting Taxpayer Information" panel discussion on April 12, 2016. The purpose of this statement is to bring to this committee's attention the importance of developing safeguards to protect the public after a data breach has been uncovered. As a matter of public record, the OPM data breach of former and present federal employees and contractors indicated that the personal and private information had been breached from the eQip system. The OPM then instituted an identity theft monitoring system designed to safeguard the victims of this data breach in the event their private information was used against them. Unfortunately, these traditional safeguards are antiquated and outdated.

Hence, cyber-criminals are far more sophisticated and have developed tools and applications to subvert the traditional methods of targeting fraud victims. Therefore, this honorable committee must consider encouraging the executive branch to consider monitoring sophisticated "shadow" and "ghost" applications that act as front-end applications that mimic official government systems. Unfortunately, during the hearing the focus was primarily a discussion about hiring industry leaders in cybersecurity to assist the agency (IRS) in protecting the taxpayer information. However, this discussion did not take into consideration the "real-world" applications of how cyber-criminals manage and process breached taxpayer data.

In closing, "shadow"' and "ghost" applications are systems that simulate official government systems, but are instead fraudulent applications. These systems are able to process millions of taxpayer dollars via bogus government letterhead ".us" domains and skewed legal jargon designed to confuse the targeted victims in banking and private industries. Hence federal government agencies must be vigilant in leading the charge against cybersecurity fraud and not just focus on the breach within the agency, but consider the sophistication of cyber-criminals that lay within and outside the federal government.