WRITTEN TESTIMONY OF
JOHN A. KOSKINEN
COMMISSIONER
INTERNAL REVENUE SERVICE
BEFORE THE
HOUSE WAYS AND MEANS COMMITTEE
SUBCOMMITTEE ON OVERSIGHT
ON THE 2016 FILING SEASON, CYBERSECURITY AND PROTECTING TAXPAYER INFORMATION
APRIL 19, 2016

PART I: UPDATE ON THE 2016 FILING SEASON

Chairman Roskam, Ranking Member Lewis and Members of the Subcommittee, thank you for the opportunity to testify today.

I am pleased to report that the 2016 filing season has gone smoothly in terms of tax return processing and the operation of our information technology (IT) systems. Through April 8 the IRS has received more than 107 million individual returns, on the way to an expected total of 150 million. We have issued more than 81 million refunds totaling more than $228 billion.

In regard to taxpayer service, the IRS saw significant improvements during this filing season over last year, largely due to additional resources provided by Congress. A total of $290 million in additional funding was approved for the IRS for Fiscal Year (FY) 2016, to improve service to taxpayers, strengthen cybersecurity and expand our ability to address identity theft, which we appreciate. This funding is the first significant increase in the IRS budget in six years and represents a positive development for the IRS and for the American taxpayer. I can assure the Congress that we are spending these resources wisely and efficiently.

We used approximately $178.4 million of this additional funding to add about 1,000 extra temporary employees to help improve our service on our toll-free phone lines. As a result, so far this filing season the telephone level of service is nearly 75 percent, which is a vast improvement over last year. The IRS has prioritized improving the level of taxpayer service on the phones during filing season, and was operating at historically low levels until the new appropriations were provided in December. When the funding for these additional employees runs out at the end of the filing season, the level of service on our phones will drop noticeably and we expect average phone services levels for the full year to be about 47 percent. This level will still be a major improvement over the 37 percent level of phone service last year. The President's 2017 Budget proposal

provides for a level of phone service above 70 percent for the full year with an investment of approximately $150 million above current levels.

Another, less visible, area of concern for us in regard to taxpayer service has been taxpayer correspondence. Typically, taxpayers correspond with the IRS after receiving a notice from the agency about an issue with their return. Our goal is to answer taxpayer correspondence within 45 days after we receive the letter.

Because of our constrained resources, we have been taking much longer to answer correspondence in recent years, though additional resources have allowed us to reduce our backlog slightly this year. However, additional improvements are needed. Our correspondence inventory is currently 923,000, with about one-third of that considered to be "over-age" – generally, unanswered after more than 45 days. The additional resources in our proposed FY 2017 budget would allow us to hire additional employees to make further improvements in this area.

During the current filing season, taxpayer demand for the services we provide online has been strong. As of April 9, we have had more than 291 million hits on our website, IRS.gov, and taxpayers have used the "Where's My Refund?" electronic tracking tool more than 254 million times. To give another example, our Online Payment Agreement application, which was streamlined and improved in 2014, has been used more than 187,000 times thus far in FY 2016.The growing demand for IRS online services underscores the need for adequate information technology and cybersecurity funding.

It is important to note that, even with the additional funding received for FY 2016, the IRS is still under significant financial constraints. This is illustrated by the fact that the IRS appropriation remains $900 million below the FY 2010 enacted level and that the $290 million increase is less than half the amount that had been requested for FY 2016 in the three critical areas mentioned above. In addition, the IRS must absorb mandated cost increases and inflation during FY 2016 that are greater than the additional funding provided.

As a result, we will need to continue the exception-only hiring policy that began in FY 2011, leaving us unable to replace most employees we lose this year through attrition. In fact, we expect the IRS workforce to continue to shrink by another 2,000 to 3,000 full-time employees during FY 2016, equaling a loss of over 17,000 since FY 2010.

While this decline in our workforce has been occurring, the number of individual returns filed grew by more than 10 million (or nearly 7 percent), from 153 million in 2010 to 163 million in 2015. Further increasing our workload, the IRS during this period has had to implement a number of significant legislative requirements, nearly all of which came with no additional funding.

For example, the IRS has worked diligently since the Affordable Care Act's enactment in 2010 to implement its tax-related provisions. Our most recent efforts began prior to the 2016 filing season, and involved preparing our systems for a reporting provision that applies to health coverage providers and certain large employers that took effect in 2015.

Another important legislative mandate is the Foreign Account Tax Compliance Act (FATCA). Most recently, implementation has involved preparing our systems to receive annual reports on accounts of U.S. taxpayers from foreign financial institutions (FFI). We currently have190,000 FFIs providing us with data under FATCA.

In FY 2016, several additional legislative mandates were put in place that carried no implementation funding with which to execute them – for example, new passport restrictions, a registration requirement for newly created 501(c)(4) organizations, and a program under which private contractors will collect taxes on some past-due accounts.

PART II: CYBERSECURITY AND PROTECTING TAXPAYER INFORMATION

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

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

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

We are aware, however, that in building toward this enhanced online experience, we must continuously upgrade and improve our authentication protocols. The reality is criminals are becoming increasingly sophisticated and are gathering vast amounts of personal information as the result of data breaches at sources outside the IRS. We must balance the strongest possible authentication

processes with the ability of taxpayers to legitimately access their data and use IRS services online. It is important to note that cybercrime (theft by unauthorized access) and privacy breaches are increasing across the country in all areas of government and industry. Cyber criminals and their methods continue to grow in sophistication, frequency, brazenness, volume and impact. IRS will continue to be challenged in our ability to maintain currency with latest technologies, processes and counter-measures.

MAKING PROGRESS AGAINST IDENTITY THEFT

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

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

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

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

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

Security Summit Group

To improve our efforts against this complex and evolving threat, the IRS held a sit-down meeting in March 2015 with leaders of the electronic tax industry, software industry and state tax officials. We agreed to build on our past cooperative efforts and find new ways to leverage our public-private partnership to help battle stolen identity refund fraud. Motivating us was the understanding that no single organization can fight this type of fraud alone.

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

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

- Summit group members identified and agreed to share 20 data components from Federal and state tax returns to improve fraud detection and prevention this filing season. For example, group members are sharing computer device identification data tied to the return's origin, as well as the improper or repetitive use of the numbers that identify the Internet "address" from where the return originates.

- Tax software providers agreed to enhance identity requirements and strengthen validation procedures for new and returning customers to protect their accounts from being taken over by criminals. This change is one of the most visible to taxpayers during the 2016 filing season, because it includes new verification procedures they need to follow to log in to their accounts. These actions will serve as the baseline for ongoing discussions and additional enhancements for the 2017 filing season.

- The Summit group created a new memorandum of understanding (MOU) regarding roles, responsibilities and information sharing pathways currently in circulation with states and industry. So far, 40 state departments of revenue and 21 tax industry members have signed the MOU, along with the IRS and endorsing organizations.

- Tax industry participants have aligned with the IRS and the states under the National Institute of Standards and Technology (NIST) cybersecurity framework to promote the protection of information technology infrastructure. The IRS and states currently operate consistently with this framework, as do many in the tax industry. Next steps in this area include follow-up sessions to develop strategy for how the NIST cybersecurity framework will be employed by all organizations within the tax industry.

- Summit group members agreed on the need to create a tax administration Information Sharing and Analysis Center (ISAC) to centralize, standardize, and enhance data compilation and analysis to facilitate sharing actionable data and information.

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

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

Identity Theft Public Awareness Campaign

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

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

As part of this public awareness campaign, the IRS, in the weeks leading up to the 2016 filing season, issued weekly tax tips describing the actions people could take to protect their data. We have updated several publications for taxpayers and tax professionals. We have posted YouTube videos on this subject, and public-awareness information is being shared online across IRS.gov, state websites and platforms used by the tax software industry and many others in the

private-sector tax community. I would note our public awareness campaign is not confined to the tax filing season, but is an ongoing effort.

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

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

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

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

VERIFYING IDENTITIES AND STOPPING SUSPICIOUS ONLINE ACTIVITY

Following the OMB Guidance and NIST Standards

The IRS continues to make every effort to ensure that we provide tax account-related services only after verifying the identity of individuals seeking those services. This is true for all of our communications channels, some of which allow

for extremely strong assurance processes that are not possible in other channels.

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

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

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

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

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

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

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

Thus, in establishing a risk assurance level to a particular online digital service, the IRS, in addition to assigning one of the four numerical levels of risk assurance, also assigns a letter representing the amount and types of validation

that a taxpayer would have to provide, in order to gain access to the digital service in question:

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

Recent Unauthorized Attempts to Access IRS Online Services

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

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

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

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

returns. As the IRS enhances return processing filters and catches more fraudulent returns at the time of filing, criminals have become more sophisticated at faking taxpayers' identities so they can evade those filters and successfully obtain fraudulent refunds.

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

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

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

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

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

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

In May 2015, the IRS announced that criminals, using taxpayer information stolen elsewhere, had been able to access the Get Transcript online application. Shortly thereafter, we disabled the application. We are now strengthening the authentication process and expect to bring the Get Transcript application back

on-line, in the near future. In reevaluating the application, we have changed the risk assurance level for this application to 3F, which will require taxpayers to undergo a multifactor authentication process in order to gain access. In the meantime, taxpayers can still place an order for a transcript online, and have it mailed to their address of record.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

LOOKING TO THE FUTURE

Building an Authentication Framework

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

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

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

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

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

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

Enhancing the Taxpayer Experience

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

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

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

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

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

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

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

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

Need for Adequate Resources and Legislative Solutions

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

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

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

- ***Cybersecurity.*** We are using approximately $95.4 million to invest in a number of critical security improvements, including more effective monitoring of data traffic and replacement of technology that supports the development, maintenance and operation of IRS applications to make processes more secure, reliable and efficient. The funding will help us to improve systems and defenses across the entire IRS, thereby helping to protect taxpayer data. We are also investing in systems to allow for enhanced network segmentation, which involves further subdividing our network, so that if any vulnerabilities occur, they would be contained to just one portion of the network.

- ***Identity Theft.*** We are using approximately $16.1million to develop advanced secure access capabilities for applications such as Get Transcript, IP PIN and others. This will also fund advanced analytics and

detection of anomalies in returns filed. In addition, this investment will allow the IRS to partner with private industry and state tax agencies through the Security Summit to, for the first time, share information systemically about suspicious activity in the tax system.

Taxpayer Service*.* As described in detail above, 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 during the filing season.

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