Supplemental Questions Submitted for the Record for Commissioner Koskinen from Senator Thune following the public hearing on June 2, 2015, "Internal Revenue Service Data Affecting Taxpayers," before the United States Senate Committee on Finance

Question 1: What has become clear is that the IRS still has a long way to go to assure Americans that their personal data is safe and secure. For example, I understand that the IRS believes that these attacks may have begun in mid-February but the IRS did not identify the problem until May. Is this accurate and, if so, why did it take so long for the IRS to identify the problem? Is the IRS taking additional steps to ensure that it can identify these types of situations earlier?

Answer: When the IRS first identified the problem with unauthorized access to information in the Get Transcript application in May, we determined that third parties with sensitive taxpayer-specific data from non-IRS sources had cleared the Get Transcript verification process on about 114,000 taxpayer accounts. In addition, it appeared at that time that third parties had made attempts that failed to pass the final verification step on about 111,000 taxpayer accounts, meaning they were unable to access account information through the Get Transcript service.

Since then, as part of the IRS's continued efforts to protect taxpayer data, the IRS conducted a deeper analysis over a wider time period covering the 2015 filing season, analyzing more than 23 million uses of the Get Transcript system. The expanded review identified an estimated additional 220,000 attempts where third parties with sensitive taxpayer-specific data cleared the Get Transcript verification process. The review also identified an additional 170,000 suspected attempts that failed to clear the authentication processes.

The IRS continues to improve its "defense-in-depth" posture by implementing technologies and processes to detect, protect against, respond to, and recover from cyber and other attacks on its IT ecosystem. Investments in IT infrastructure, network security, data security and loss prevention, cyber analytics and monitoring, cyber preparedness, and secure taxpayer access are all key to improving this posture. Among other important cybersecurity priorities, the IRS is currently focused on:

- Replacement of prioritized backlog of aged and obsolete infrastructure components, including aged servers and infrastructure software, which are introducing security risks, excessive system downtime, and incompatibilities across systems and programs.

- Replacement of aged network infrastructure that is not in compliance with Homeland Security Presidential Directive-12 (HSPD-12), as well as implementation of a network segmentation solution to restrict IRS local area network (LAN) access to users and devices based on pre-determined authorization levels, to enhance protection of our sensitive data and enhance the IT security posture on our networks.

- Implementation of advanced analytics and fraud detection capabilities within the IRS Integrated Enterprise Portal and authentication environments to better protect access to the taxpayer accounts and other taxpayer-facing applications, including new tools to detect and block suspicious IP addresses, enhanced data logging capability, better data analytic tools and capabilities, and enhanced network perimeter security surveillance.

The IRS launched a more rigorous authentication process for taxpayers on June 7, 2016, with the assistance of top digital experts at the U.S. Digital Service. This system will significantly increase protection against identity thieves impersonating taxpayers using the IRS Get Transcript online service. This enhanced authentication process is now also being used with our Identity Protection PIN application and will provide a foundation for additional IRS self-help services in the future.

Question 2: As you note in your testimony, a key element of data security is authentication. In fact, you note that authentication protocols need to become more sophisticated.

Can you briefly discuss how these cybercriminals were able to access information that would typically only be known to the taxpayer? How does the IRS intend to stay one step ahead of criminal syndicates given what you have learned from this very unfortunate incident?

Answer: In addition to a general increase in sophistication, criminals are gathering vast amounts of personal information stolen through commercial and government data breaches at sources outside the IRS. Criminal organizations invest in acquiring personal information similar to any other business in a competitive market. Previously, sensitive information such as shared secrets would have been acquired through physically stealing private records. However, the proliferation of easily accessible information about individuals in the past few years means that previously private sensitive information is often available from criminal organizations for a fee, thus undermining long-standing authentication techniques.

The IRS has taken a multi-pronged approach which includes:

- Strengthening our internal protocols, as evidenced by the recent re-launch of Secure Access with multi-factor authentication and stronger identity proofing in partnership with USDS;
- Partnering with industry through the Security Summit as we jointly implement the enhanced authentication data elements and the information sharing and assessment center;
- Continuing to engage the broader tax administration "ecosystem" as we see track shifts in criminal behavior and emerging vulnerabilities.

The IRS cannot do this alone. The solution requires support from individuals and from companies, by protecting the taxpayer information in their hands (before it becomes federal tax information) through adequate identity proofing, authentication, and cybersecurity controls. The IRS intends to continue our dialogue with the National Institute of Standards and Technology about standards that can help improve security while also focusing on cost, time-to-market, and the need to serve all taxpayers.

Question 3: One approach to data security that the IRS is testing is the Identity Protection Personal Identification Number, or IP PIN. You state in your testimony that the IRS has already issued 1.5 million IP PINs to taxpayers for the 2015 filing season and that any taxpayer in Florida, Georgia or Washington, D.C. can apply to receive an IP PIN.

Can you explain how the IP PIN works and whether the IRS views this program as a potential solution to identity-theft related tax fraud? Do you intend to quantify how much potential refund fraud is prevented by this program?

Answer: The Identity Protection Personal Identification Number (IP PIN) is a unique 6-digit identifier assigned to eligible taxpayers to help prevent the misuse of their Social Security numbers on fraudulent federal income tax returns; we use the IP PIN to authenticate a return filer as the legitimate taxpayer at the time a return is filed. Taxpayers can receive an IP PIN if they meet any of the following criteria:

- They were a victim of tax related identity theft. As a result their accounts are marked with an identity theft indicator and a notice is issued to them in December or early January containing their IP PIN.
- They filed their last tax return as a resident of Florida, Georgia, or District of Columbia, three areas where there have been particularly high

concentrations of stolen identity refund fraud, and elected to participate in a pilot program offering IP PINs.

- They received a letter identifying them as victims of identity theft and inviting them to "opt in" to obtain an IP PIN.

Once a taxpayer receives an IP PIN, the taxpayer must use the IP PIN to confirm his or her identity on any federal tax return, current or delinquent, filed during the calendar year. Safeguards in the IP PIN assignment process ensure an IP PIN cannot be used in more than one filing season. The IRS mails new IP PINs to taxpayers each year before the start of the filing season and taxpayers must use them on any returns filed during that year.

Taxpayers who need to retrieve a lost IP PIN can use an online tool to do so. On July 19, 2016 the "Get an IP PIN" tool returned to IRS.gov with the same Secure Access protocol as our Get Transcript application. The re-launched tool uses a multi-factor authentication process that will help protect taxpayers and prevent fraud. Taxpayers must verify their identities using a more rigorous Secure Access process that requires them to have immediate access to an email address, account information from a credit card or other loans types and a text-enabled mobile phone. New and returning users must follow the Secure Access steps outlined in Fact Sheet 2016-20, How to Register for Get Transcript Online Using New Authentication Process.

If a return is e-filed with a taxpayer's SSN and the IP PIN is missing or incorrect, our system will reject it for the taxpayer's protection. Filing a paper return with a missing or incorrect IP PIN will delay processing while we determine that it's the taxpayer's return. The IP PIN is one piece in the IRS arsenal to combat identity theft and fraud. We continue to monitor the effectiveness of the IP PIN, the IP PIN assignment process, and the related customer service options. In an effort to use the IP PIN proactively, we are currently assessing our IP PIN strategy and conducting a usage study. We will consider data- and policy-based decisions to expand or alter the program once the study is completed. In addition to the study, teams formed as a result of the Security Summit are looking at strengthening authentication at the point of filing and the IP PIN is a component of that strategy.

In an effort to gauge taxpayer interest, we conducted a pilot to offer the IP PIN in three states with high concentrations of stolen identity refund fraud: Georgia, Florida and the District of Columbia. The pilot found that only a small percentage of the eligible population was using an IP PIN.

Although additional expansion of the IP PIN program should help safeguard more taxpayers from tax-related identity theft and refund fraud, it would require a substantial investment of financial resources at a time when reductions in our budget have stretched resources across the agency. As stated above, we are conducting research analysis to determine the feasibility of expanding the IP PIN program while also exploring other tools and solutions to increase security of taxpayer data available to a wider cross section of taxpayers. The Congress can help protect taxpayers and their identities by fully funding the FY 2017 President's Budget request for the IRS and the Treasury-wide Cybersecurity Enhancement Account. These requested resources will allow the IRS to continue to develop authentication capabilities and access controls required to expand the use of mobile devices, cloud computing, and collaborative technologies. This project will fund the design and implementation of a common service to verify user identity, register individuals, and provide and validate their credentials Within current budget constraints, we are committed to doing all that we can to prevent the payment of fraudulent refunds, pursue the perpetrators, and assist the victims.

Question 4: One of the recommendations in the Administration's budget that you refer to in your testimony is the proposal to move up the date when employers must file W-2 info to January 31, which is prior to the start of the tax filing season. However, as you know, W-2s are filed by employers with the Social Security Administration, not the IRS.

As such, does the IRS have the systems in place to get this information from the Social Security Administration in a timely manner? If W-2s had been filed with the SSA by the end of January, would it have prevented the 13,000 fraudulent refunds worth roughly $39 million that the IRS believes relate to this latest data breach?

Answer: The Administration's budget proposal to move up the date when employers must file Forms W-2, *Wage & Tax Statement,* with the Social Security Administration (SSA) was enacted as a part of the Protecting Americans from Tax Hikes Act (PATH), Section 201(a). This provision accelerates the filing date for Forms W-2 to January 31, beginning with forms filed in 2017. Under prior law, Forms W-2 had to be filed by the end of March, if sent electronically, or before the end of February, if submitted on paper. SSA processes the Forms W-2 and then transmits the information from the forms to the IRS daily starting in mid-January following the close of the prior tax year. The SSA and IRS have a strong long-standing partnership and memorandum of understanding for this data transfer.

Although the filing season for individual taxpayers generally begins before the Form W-2 deadline, the IRS will use the early-filed Forms W-2, along with other detection methods to assist in preventing the possible payment of fraudulent refunds. In addition to using the Forms W-2 filed earlier as a result of the PATH Act, we will leverage the Accelerated Information Reporting Program by which many payroll reporting agents (or payroll service providers) send their clients' Form W-2 data directly to the IRS at the same time they send it to the SSA.

The receipt of earlier Forms W-2 is a valuable tool in our identity theft detection and prevention strategy. Third-party information returns, such as Forms W-2, serve an increasingly important role in preventing tax return based identity theft and refund fraud before tax refunds are issued. The introduction of more Form W-2 data into our tax return screening strategy earlier in the filing season will enhance the IRS's ability to perform risk-based analysis of returns to identify cases of potential identity theft and refund fraud before refunds are issued, further strengthening pre-refund processing defenses. Although the earlier filing of Forms W-2 alone will not prevent all identity-theft refunds, it is a valuable tool in evaluating returns and could have helped identify inconsistencies on returns related to the Get Transcript incident.

Question 5: TIGTA has reported that it has made 44 recommendations to the IRS in the area of information security that the IRS has yet to implement. Does the IRS intend to implement all of these recommendations and, if so, on what timeline?

Answer: The IRS has currently implemented 35 of the 44 recommendations. The remaining 9 recommendations will be implemented and closed by early 2017.