COMMITTEE ON WAYS AND MEANS

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515

May 28, 2015

The Honorable John Koskinen
Commissioner
Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20224

Dear Commissioner Koskinen:

Taxpayer confidence in the Internal Revenue Service's (IRS) ability to safeguard personal information is critical to our nation's system of voluntary tax compliance. The IRS's announcement[1] that cyber attackers took advantage of IRS system vulnerabilities to access 104,000 taxpayers' confidential information is a profound mission failure. We are writing to inquire about the full extent of the breach, including whether these crimes were facilitated by known system weaknesses and what steps the IRS is taking to prevent any further breaches.

In recent months, both the Treasury Inspector General for Tax Administration (TIGTA) and the Government Accountability Office (GAO) identified significant deficiencies in the IRS's information security systems. In particular, they found that the IRS's systems did not have appropriate identity and access management (IA&M), leaving them vulnerable to cyber attacks, including unauthorized access to personally identifiable information. Further, they found that the systems had weak configuration management, which would prevent administrators from monitoring and controlling changes to IRS IT systems.

On May 26, 2015, the IRS announced that its online Get Transcript service, established in January 2014, had been exploited, providing improper access to 104,000 taxpayers' confidential information. The IRS reported that before it detected the unauthorized access, it issued 15,000 fraudulent refunds, totaling

[1] IRS Statement on the "Get Transcript" Application, May 26, 2015, *available at* http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application

about $50 million. Until now, the IRS has been promoting its Get Transcript application nationally as providing safe and streamlined customer service.[2]

But in its review of the IRS's information systems, TIGTA found that for FY 2014, the IRS was fully compliant with fewer than half of the performance metrics established by the Federal Information Security Management Act of 2002 (FISMA).[3] FISMA establishes a clear framework for how government agencies must protect information and information systems, support the safe and secure adoption of new technology, and create a sophisticated information security workforce.[4] It is essential that the IRS maintains FISMA standards to protect taxpayer information, but TIGTA reported that only five of eleven security areas met all FISMA requirements. Two key areas—configuration management and identity and access management—failed to meet the majority of standards needed for compliance.

Strong configuration management is important because it creates stability and efficiency within a system and allows administrators to identify and address problems quickly. Appropriate IA&M is key to preventing cyber attacks because it ensures that only people with proper identification and authentication may access systems. Weak IA&M can leave systems vulnerable to cyber attacks, including social engineering, and can make it difficult or impossible to identify whether unintended users are accessing information within the system.

Similarly, in March 2015, GAO released a report highlighting numerous weaknesses in the IRS's systems. GAO found that the IRS did not have strong password protection controls; IRS employees had excessive access privileges that allowed them to see information not necessary for their jobs; and physical access controls were inconsistent. Additionally, the IRS's servers used weak encryption—or no encryption at all—to authenticate users, potentially allowing unauthorized users to view data and then use that information to gain access to the systems.[5]

Both GAO and TIGTA have reported that these weaknesses leave taxpayer information vulnerable to attack. TIGTA concluded that:

> *[U]ntil the IRS takes steps to improve its security program deficiencies and fully implements all 11 security program areas required by the FISMA, taxpayer*

[2] *See* Commissioner Koskinen's Remarks to the National Press Club, April 2, 2014, *available at* http://www.irs.gov/uac/Newsroom/Prepared-Remarks-of-Commissioner-of-Internal-Revenue-Service-John-Koskinen-before-the-National-Press-Club-2014.

[3] TIGTA, Federal Information Security Management Act Report for FY 2014, Sept. 2014.

[4] Office of Management and Budget, Annual Report to Congress: Federal Information Security Management Act, May 2014.

[5] GAO, Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data, March 2015.

> *data will remain vulnerable to inappropriate use, modification, or disclosure, possibly without being detected.*[6]

GAO's findings matched TIGTA's conclusions:

> *Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks . . . threats include the ever-growing number of cyber-based attacks that can come from a variety of sources—individuals, groups, and countries who wish to do harm.*[7]

These security safeguards are extremely important, especially as the government relies more and more on information technology.

The IRS has a responsibility to protect taxpayer information from unauthorized access and attacks. Clearly, the agency needs to do more. In order for the House Ways and Means Committee to better understand the breach that resulted in 104,000 taxpayers' information being compromised and the steps the IRS is taking to prevent future unauthorized disclosures, please respond to the following questions by June 11, 2015:

1) Describe the IRS's Get Transcript application generally, as well as any other systems affected by the cyber attack.

2) When and how did the IRS discover the cyber attack? Did any IRS detection involve algorithmic analysis, including analysis of account access patterns, transcript request trends, number or frequency of password reset attempts, etc.? If so, please describe the indicators detected and how IRS systems are designed to screen for them.

3) Did the IRS discover the problems itself, or did another organization or person call the problems to the IRS's attention? If so, who, when, and how did they inform the IRS?

4) We understand that 104,000 taxpayers' information was compromised. Were the 104,000 taxpayers part of a discrete group, or were they a random selection from the pool of taxpayers?

[6] TIGTA, Federal Information Security Management Act Report for FY 2014, Sept. 2014.

[7] GAO, Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data, March 2015.

5) What data were accessed by the attackers?

6) Is the IRS assured that no other taxpayers' information, beyond those identified above, was compromised? If so, how?

7) Is the IRS reviewing its other applications, such as Where's My Refund, IRS Direct Pay, and IRS Online Payment Agreement, to determine if they are vulnerable or have been subject to an attack?

8) What steps is the IRS taking to notify potential victims of the attack?

9) What determinations has the IRS made about the cause of the attack? Who carried out the attack? What vulnerabilities allowed the attack to occur?

10) The IRS has reported that the criminals who carried out the attacks were able to answer "out of wallet" questions in order to access the system. What types of "out of wallet" questions does the IRS use to verify taxpayers? What steps will the IRS take to strengthen its authentication of users?

11) What steps will the IRS take to protect the 104,000 accounts from further unauthorized access or related crimes, such as identity theft related tax fraud?

12) Is the IRS coordinating with other agencies to investigate the attack and/or prevent taxpayer information from being used to perpetuate fraud in other federal programs? If yes, please describe all coordination efforts.

13) Please provide all information on any improvements the IRS has made to its information security to address TIGTA's and the GAO's recommendations.

14) Please provide a summary of any outstanding information security weaknesses, including any current agency efforts to resolve them and/or future plans to resolve them.

Additionally, please provide a briefing for Ways and Means Oversight Subcommittee staff on the cyber attack, no later than June 12, 2015.

Thank you for your attention to this extremely important matter. If you have any questions about this request, please do not hesitate to contact Oversight Subcommittee staff at (202) 225-5522.

Sincerely,

PAUL D. RYAN
Chairman
Committee on Ways and Means

PETER J. ROSKAM
Chairman
Subcommittee on Oversight