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

HEARING CHARTER

Can the IRS Protect Taxpayers' Personal Information?

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

Purpose

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

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

Witness List

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

---

[1] Brian Krebs, "IRS Suspends Insecure 'Get IP PIN' Feature," Krebs on Security, March 16, 2016, available at: http://krebsonsecurity.com/2016/03/irs-suspends-insecure-get-ip-pin-feature.
[2] "Electronic Authentication Guideline," NIST Special Publication 800-63-2, August 2013, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf.
[3] Ibid.
[4] "E-Authentication Guidance for Federal Agencies," OMB Memorandum M-04-04, December 16, 2003, available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.

Background

Get Transcript

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

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

IP PIN

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

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

---

[5] Fact Sheet: Education Datapalooza to Promote Innovation in Improving College Access, Affordability, and Completion, January 15, 2014, available at: https://www.whitehouse.gov/sites/default/files/docs/datapalooza_fact_sheet.pdf.

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

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

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

[9] "There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft," TIGTA Report, July 19, 2012, Reference Number: 2012-42-080, available at: https://www.treasury.gov/tigta/auditreports/2012reports/201242080fr.html.

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

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

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

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

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

Treasury Inspector General for Tax Administration (TIGTA) Report

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

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

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

U.S. Government Accountability Office (GAO) Report

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

---

[13] Brian Krebs, "Thieves Nab IRS PINs to Hijack Tax Refunds," Krebs on Security, March 16, 2016, available at: http://krebsonsecurity.com/2016/03/thieves-nab-irs-pins-to-hijack-tax-refunds.
[14] IRS Statement, March 7, 2016, available at: https://www.irs.gov/uac/Newsroom/IRS-Statement-on-IP-PIN.
[15] "Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures are Needed," TIGTA Report, November 19, 2015, Reference Number: 2016-40-007, available at: https://www.treasury.gov/tigta/auditreports/2016reports/201640007fr.pdf.
[16] Ibid.
[17] Ibid.
[18] Ibid.
[19] "Information Security: IRS Needs to Further Improve Controls Over Financial and Taxpayer Data," GAO Report, March 2016, GAO-16-398, available at: http://www.gao.gov/assets/680/676097.pdf.
[20] Ibid.

The report further notes that:

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

Unless IRS takes steps to follow GAO's recommendations, "its financial and taxpayer data will remain unnecessarily vulnerable to inappropriate and undetected use, modification, or disclosure."[22]

[21] Ibid.
[22] Ibid.