WRITTEN TESTIMONY OF
EDWARD T. KILLEN
CHIEF PRIVACY OFFICER
AND
SILVANA GINA GARZA
CHIEF INFORMATION OFFICER
INTERNAL REVENUE SERVICE
BEFORE THE
HOUSE WAYS AND MEANS COMMITTEE
SUBCOMMITTEE ON OVERSIGHT
ON IRS TAXPAYER AUTHENTICATION EFFORTS
SEPTEMBER 26, 2018

INTRODUCTION

Chairman Jenkins, Ranking Member Lewis, and Members of the Subcommittee, thank you for the opportunity to discuss the IRS's taxpayer authentication processes as they support our overall data protection efforts.

Securing our systems and taxpayer data continues to be a top priority for the IRS. First, the IRS works continuously to protect our computer systems from cyber incidents, intrusions and attacks. They remain secure through a combination of cyber defenses, which currently withstand about an average of 2 ½ million attempts a day to access our systems. Many of these attempts are sophisticated in nature or represent advanced persistent threats. Second, the IRS is waging an ongoing battle to protect taxpayers and their information against the growing problem of identity theft, particularly tax refund fraud, for which cybercriminals frequently exploit vast amounts of data from breaches outside the tax system.

One of the critical components of the IRS's efforts to secure our systems and protect taxpayer data involves continuously working to improve our processes for authenticating the identities of taxpayers who interact with the agency through our service channels, including in-person, over the phone and online. Over the last several years, we particularly focused on strengthening our online authentication processes, and we have made critical progress in this area.

However, the cyber landscape is ever changing. Efforts to steal taxpayer data and infiltrate our systems, by cybercriminals with access to cutting-edge technology, resources and new methods, continue to grow in sophistication, frequency, brazenness, volume and impact. As a result, the risks associated with sophisticated cybersecurity threats are increasing. This is confirmed by the growing incidence of cybercrime (theft by unauthorized access) and privacy breaches we are seeing across the country in all areas of government and industry. Remaining current with the latest technologies, processes and counter-measures will continue to challenge the IRS, but we will work diligently to strengthen data protections as we expand online services and applications for taxpayers.

SAFEGUARDING IRS SYSTEMS AND TAXPAYER DATA

The IRS has made significant progress over the last several years in protecting taxpayers and the tax system against tax-related identity theft. A major contributor to this progress is the work being done by the Security Summit, a unique partnership that includes the IRS, tax industry leaders and state tax commissioners. This partnership, in combination with our fraud detection systems, is making a difference. In fact, the 2018 filing season was the third in which the IRS worked with our Security Summit partners to put in place many protections to help stop fraudulent returns from entering tax processing systems.

I'm pleased to report recent statistics show a continuing and substantial decline in several indicators of tax-related identity theft. From 2015 to 2017, the number of taxpayers reporting to the IRS that they were victims of identity theft dropped by 65 percent, and the number of tax returns with confirmed identity theft fell by 57 percent with more than $20 billion in taxpayer refunds being protected.

An important part of the Summit's work has involved sharing information, especially leads on emerging identity theft schemes. Toward that end, in 2017 the Summit partners created the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC), which has helped Summit partners to rapidly share information and the IRS to identify emerging schemes. Sharing information and doing it in a timely manner is critical to our ability to respond rapidly to evolving threats, so the ISAC will be an important tool going forward.

We realize we cannot let up in the fight against fraud and tax-related identity theft. As we have strengthened our defenses, identity thieves are continuously working to obtain more-detailed financial information to help them do a better job of impersonating legitimate taxpayers and file more realistic-looking tax returns to claim fraudulent refunds.

Cyberthieves are targeting tax professionals, human resources departments, businesses and other places with large amounts of sensitive financial information. Therefore, the IRS and its partners not only continue to improve our safeguards against fraudulent returns, but we also continue to encourage taxpayers, tax professionals and businesses to protect their data and avoid becoming victims of proliferating tax scams.

AUTHENTICATION PROCEDURES AND ONGOING IMPROVEMENTS

A major component of the IRS's efforts to protect taxpayer data and combat cyber fraud and tax-related identity theft involves our authentication procedures for online transactions. The IRS makes every effort to ensure that we provide tax account-related services only after verifying the identity of individuals seeking those services – whether this inquiry is on-line, in-person, or via telephone. For the last several years, we have been working to improve our authentication processes and procedures, including the development of a strong, coordinated and evolving authentication framework.

In 2015, the IRS established the Identity Assurance Office to help us better understand authentication and fraud detection needs across the agency. The following year, the Identity Assurance Office issued its IRS Identity Assurance Strategy and Roadmap. The Strategy and Roadmap includes core objectives, priority campaigns and foundational initiatives designed to meet both short- and long-term needs to strengthen the IRS's identity assurance posture. This guiding document has been essential in putting the IRS on a path to more robust omni-channel taxpayer authentication procedures, online capabilities and services. As this field continues to evolve dynamically, with the pace of technological changes and the risks associated with sophisticated cybersecurity threats, we will continue to update this document to ensure it addresses current IRS needs and reflects state-of-the-art technological capabilities and evolving federal requirements.

Secure Access System

The IRS employs differing Levels of Assurance among the various digital services used by taxpayers, according to the risk involved. For example, the level of assurance required for an online tool that only accepts payments from a taxpayer can reasonably be set lower than an application that provides taxpayers access to their personal tax information.

The IRS took an important step forward in safeguarding high-risk transactions in 2016 when it implemented the Secure Access e-Authentication system, a rigorous identity verification process that helps protect the IRS's online tools in two ways. First, it has a strong identity-proofing process, which helps establish that first-time users are who they say they are. Second, it requires returning users to authenticate and go through a two-factor access process by entering their username and password plus a security code. The security code can be sent via text message to their mobile phone, or as a more secure option, can be generated by the IRS2Go mobile app. This two-factor authentication process met the federal standards for protecting information that were recently superseded by the new National Institute of Standards and Technology (NIST) guidelines. We are now evaluating how to comply with the new standards (NIST 800-63-3), as we explain in greater detail below.

Overall, the IRS takes a risk-based approach to evaluating the level of security required based on federal guidelines. Since implementing Secure Access, the IRS has analyzed each online application we offer to taxpayers and tax professionals, and the types of transactions those applications enable, to identify the applications that require the highest levels of authentication.

The first applications we migrated to Secure Access were the most critical services and applications – ones that provide users with sensitive information. Those include, for example, obtaining prior-year tax information using the Get Transcript Online application, looking up an Identity Protection Personal Identification Number, and accessing the taxpayer's online IRS account. We have continued to migrate other online tools to the Secure Access system as appropriate. We took a major step in December 2017 when we extended Secure Access protections to e-Services, which is a suite of online tools for tax professionals, including electronic filing, transcript delivery systems and taxpayer identification number matching. This was especially important because these tools access sensitive data, and because cybercriminals increasingly target tax professionals.

The IRS will continue to look carefully at how taxpayers interact with our online web applications and make improvements where needed. This focus on the user experience applies not only to online applications, but also to other service channels where the IRS continues to hear the voice of the customer to drive service improvements.

OMB and NIST Standards

The IRS is committed to continuously improving our authentication procedures in line with guidelines from the Office of Management and Budget (OMB) and NIST, which apply to all federal agencies implementing digital identity services. Over the past year, the IRS performed an in-depth analysis of all its secure online applications used by taxpayers and tax professionals. Our goal was to ensure we employed adequate security controls. Where necessary, we implemented strong mitigations and compensating controls to strengthen the overall security of online services. Through our analysis, we confirmed that applications behind Secure Access were fully compliant with the guidelines outlined in NIST Special Publication (SP) 800-63-2.

As noted above, NIST revised its guidelines in June 2017 with the release of NIST SP 800-63-3. This was a complete rewrite of the eAuthentication standard, and creates a new framework for federal agencies to improve the security of their identity-proofing and authentication programs. The new guidelines introduce new concepts and redefine how federal agencies implement digital identity services. Further, the new standard has substantially more rigorous requirements than the previous standard. The IRS is working to assess how the new guidelines affect the processes and systems that taxpayers use, and we have taken preliminary steps to implement the guidelines. For example, we developed a comprehensive, data-driven approach to assess applications against the new NIST guidelines and have begun testing the new process.

One of the first steps we took was to determine the extent to which existing applications might meet the new NIST standards. For example, we assessed the current Secure Access system against the new NIST guidelines. We found the IRS meets Authentication Assurance Level (AAL) 2 and Identity Assurance Level (IAL) 1 requirements. However, like all federal agencies, the IRS faces challenges implementing the new NIST standards. As they enter the market, new products and services must be certified by the appropriate credentialing authorities. We understand that this work is ongoing. In effect, commercially-available solutions that meet the new, more stringent requirements are not yet widely available. Despite these challenges, the IRS continues to pursue a secure digital experience for all users.

Monitoring Suspicious Activity

Another aspect of ensuring that only authorized users access taxpayer data in our systems involves our efforts to monitor, detect and analyze suspicious activity in those systems. As the IRS has improved its procedures for authenticating users of our online services, we have also enhanced network monitoring controls to help block suspicious activity on IRS.gov, and thus thwart cybercriminals' attempts to obtain unauthorized access to taxpayer data through our online applications. However, the cyber landscape is consistently shifting, requiring stronger authentication requirements and robust cyber monitoring tools; which has increased costs for programs.

In a report earlier this year, the Treasury Inspector General for Tax Administration (TIGTA) noted that the IRS has made progress toward implementing effective network monitoring controls, and the controls now in place provide a significant improvement in the IRS's ability to detect and prevent cyberattacks. At the same time, we acknowledge that the IRS has more work to do in this area. We agree with all of the recommendations for improvement TIGTA made in its report and are working to address each one.

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