United States Government Accountability Office

Testimony

Before the Committee on Finance, United States Senate

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, April 12, 2016

INFORMATION SECURITY

IRS Needs to Further Improve Controls over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud

Statement of Gene L. Dodaro
Comptroller General of the United States

GAO Highlights

Highlights of GAO-16-589T, a testimony before the Committee on Finance, U.S. Senate

April 12, 2016

INFORMATION SECURITY

IRS Needs to Further Improve Controls over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud

Why GAO Did This Study

In collecting taxes, processing returns, and providing taxpayer service, IRS relies extensively on computerized systems. Thus it is critical that sensitive taxpayer and other data are protected. Recent data breaches at IRS highlight the vulnerability of taxpayer information. In addition, identity theft refund fraud is an evolving threat to honest taxpayers and tax administration. This crime occurs when a thief files a fraudulent return using a legitimate taxpayer's identity and claims a refund. In 2015, GAO added identity theft refund fraud to its high-risk area on the enforcement of tax laws and expanded its government-wide high-risk area on federal information security to include the protection of personally identifiable information.

This statement discusses (1) IRS information security controls over financial and tax processing systems, (2) IRS actions to address identity theft refund fraud, and (3) the status of selected IRS filing season operations. This statement is based on previously published GAO work as well as an update of selected data.

What GAO Recommends

In addition to 49 prior recommendations that had not been implemented, GAO made 45 new recommendations to IRS to further improve its information security controls and the implementation of its agency-wide information security program. GAO has also made recommendations to help IRS combat identity theft refund fraud, such as assessing costs, benefits, and risks of taxpayer authentication options.

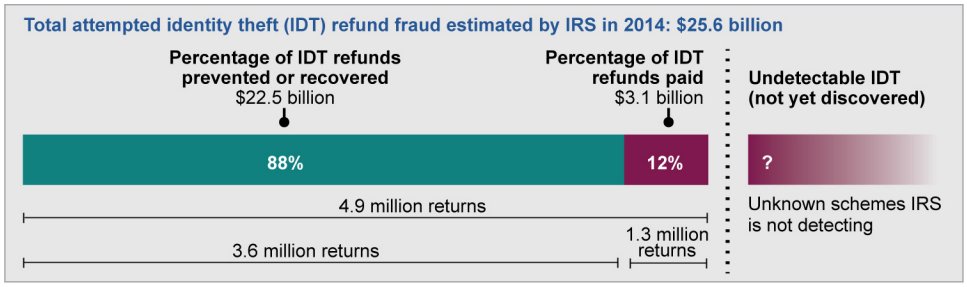
View GAO-16-589T. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, James R. McTigue, Jr. at (202) 512-9110 or mctiguej@gao.gov or Jessica K. Lucas-Judy at (202) 512-9110 or LucasJudyJ@gao.gov .

What GAO Found

In March 2016, GAO reported that the Internal Revenue Service (IRS) had instituted numerous controls over key financial and tax processing systems; however, it had not always effectively implemented other controls intended to properly restrict access to systems and information, among other security measures. In particular, while IRS had improved some of its access controls, weaknesses remained in key controls for identifying and authenticating users, authorizing users' level of rights and privileges, encrypting sensitive data, auditing and monitoring network activity, and physically securing facilities housing its IT resources. These weaknesses were due in part to IRS's inconsistent implementation of its agency-wide security program, including not fully implementing prior GAO recommendations. GAO concluded that these weaknesses collectively constituted a significant deficiency for the purposes of financial reporting for fiscal year 2015. As a result, taxpayer and financial data continue to be exposed to unnecessary risk.

Identity theft refund fraud also poses a significant challenge. IRS estimates it paid $3.1 billion in these fraudulent refunds in filing season 2014, while preventing $22.5 billion (see figure). The full extent is unknown because of the challenges inherent in detecting this form of fraud.

IRS Estimates of Attempted Identity Theft Refund Fraud, 2014



Source: GAO analysis of IRS data. | GAO-16-589T

IRS has taken steps to combat identity theft refund fraud such as improving phone service for taxpayers to report suspected identity theft and working with industry, states, and financial institutions to detect and prevent it. However, as GAO reported in August 2014 and January 2015, additional actions can further assist the agency in addressing this crime, including pre-refund matching of taxpayer returns with information returns from employers, and assessing the costs, benefits, and risks of improving methods for authenticating taxpayers. In addition, the Consolidated Appropriations Act 2016 includes a provision that would help IRS with pre-refund matching and also includes an additional $290 million to enhance cybersecurity, combat identity theft refund fraud, and improve customer service.

According to IRS and industry partners, the 2016 filing season has generally gone smoothly, with about 95 million returns and $215 billion in refunds processed through April 1, 2016. In addition, IRS increased its level of phone service to taxpayers, although it has not developed a comprehensive strategy for customer service as GAO recommended in December 2015.

Chairman Hatch, Ranking Member Wyden, and Members of the Committee:

Thank you for the opportunity to testify on cybersecurity and protecting taxpayer information. As taxpayers file their returns for 2015, it is especially important that the Internal Revenue Service (IRS) ensure that adequate protections are in place to secure the sensitive information entrusted to the agency by members of the public.

The federal government faces an evolving array of cyber-based threats to its systems and data. Reported incidents and data breaches at federal agencies, including IRS, have affected millions of people through the compromise of sensitive personal information and underscore the continuing and urgent need for effective information security. We initially designated federal information security as a government-wide high-risk area in 1997, and in 2003 we expanded this area to include computerized systems supporting the nation's critical infrastructure. In 2015 we added the protection of personally identifiable information (PII)[1] that is collected, maintained, and shared by both federal and nonfederal entities.[2]

In carrying out its mission to collect taxes, process tax returns, and enforce U.S. tax laws, IRS relies extensively on computerized systems and on information security controls to protect the confidentiality, integrity, and availability of sensitive personal and financial information for each U.S. taxpayer. Recent information security incidents at IRS further highlight the importance of ensuring that these controls are effectively implemented.

As you know, the filing season is the time when most taxpayers interact with IRS. As in previous years, a major challenge during the filing season is protecting taxpayers' information and addressing identity theft (IDT) refund fraud, which occurs when a refund-seeking fraudster obtains an individual's Social Security number, date of birth, or other PII and uses it to file a fraudulent tax return seeking a refund.[3] This crime burdens

[1]PII is information about an individual, including information that can be used to distinguish or trace their identity, such as name, Social Security number, mother's maiden name, or biometric records, as well as any other personal information that is linked or linkable to an individual.

[2]See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[3]This statement discusses IDT refund fraud and not employment fraud. IDT employment fraud occurs when an identity thief uses a taxpayer's name and Social Security number to obtain a job.

honest taxpayers because authenticating their identities is likely to delay processing their returns and refunds. Moreover, the victim's PII can potentially be used to commit other crimes. Given current and emerging risks, in 2015 we expanded the enforcement of our tax laws high-risk area to include IRS's efforts to address IDT refund fraud.[4]

My statement today focuses on opportunities to assist IRS in addressing (1) information security weaknesses we have identified and (2) the challenge of identity theft refund fraud. I will also discuss the status of selected IRS filing season operations.

Within the context of my testimony, it is important to note that, for fiscal year 2016, IRS received about $290 million in additional funding to support these areas. Specifically, the funding was intended to improve customer service, IDT identification and prevention, and cybersecurity efforts.[5] According to IRS's spending plan this funding will be used to invest in (1) increased telephone level of service, including reduced wait times and improved performance on IRS's Taxpayer Protection Program/Identity Theft Toll Free Line ($178.4 million); (2) cybersecurity including network security improvements, protection from unauthorized access, and enhanced insider threat detection ($95.4 million); and (3) IDT refund fraud prevention ($16.1 million).

My statement is based in part on our previous reports issued between August 2014 and March 2016. We updated selected data in this statement with 2016 data from IRS on individual income tax return processing and telephone service, as well as IRS's fiscal year 2016 spending plan for the additional $290 million in appropriated funds. We also incorporated IRS statements on recent data breaches and IRS actions to address our past recommendations. To assess data reliability, we reviewed IRS data and documentation and assessed documentation for data limitations. We found the data to be sufficiently reliable for our purposes. All the work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that

[4]GAO-15-290.

[5]Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. E, § 113, 129 Stat. 2242 (Dec. 18, 2015).

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

IRS's mission is to provide America's taxpayers top-quality service by helping them to understand and meet their tax responsibilities and to enforce the law with integrity and fairness to all. During fiscal year 2015, IRS collected more than $3.3 trillion; processed more than 243 million tax returns and other forms; and issued more than $403 billion in tax refunds. IRS employs about 90,000 people in its Washington, D.C., headquarters and at more than 550 offices in all 50 states, U.S. territories, and some U.S. embassies and consulates. Each filing season IRS provides assistance to tens of millions of taxpayers over the phone, through written correspondence, online, and face-to-face. The scale of these operations alone presents challenges.

In carrying out its mission, IRS relies extensively on computerized information systems, which it must effectively secure to protect sensitive financial and taxpayer data for the collection of taxes, processing of tax returns, and enforcement of federal tax laws. Accordingly, it is critical for IRS to effectively implement information security controls and an agency-wide information security program in accordance with federal law and guidance.[6]

Cyber incidents can adversely affect national security, damage public health and safety, and compromise sensitive information. Regarding IRS specifically, two recent incidents illustrate the impact on taxpayer and other sensitive information:

- In June 2015, the Commissioner of the IRS testified that unauthorized third parties had gained access to taxpayer information from its Get Transcript application.[7] According to officials, criminals used taxpayer-

[6]In particular, the Federal Information Security Modernization Act of 2014 (FISMA), among other things, requires the head of each agency to provide information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the agency's information or information systems. Pub. L. No. 113-283, § 2(a), 128 Stat. 3074 (Dec. 18, 2014), codified at 44 U.S.C. § 3554(a).

[7]This application provides users, via the IRS website, the ability to view, print, and download tax account, tax return, and record of account transcripts; wage and income documents; and proof of non-filing transcripts.

specific data acquired from non-department sources to gain unauthorized access to information on approximately 100,000 tax accounts. These data included Social Security information, dates of birth, and street addresses. In an August 2015 update, IRS reported this number to be about 114,000, and that an additional 220,000 accounts had been inappropriately accessed. In a February 2016 update, the agency reported that an additional 390,000 accounts had been accessed. Thus, about 724,000 accounts were reportedly affected. The online Get Transcript service has been unavailable since May 2015.

- In March 2016, IRS stated that as part of its ongoing security review, it had temporarily suspended the Identity Protection Personal Identification Number (IP PIN) service on IRS.gov. The IP PIN is a single-use identification number provided to taxpayers who are victims of identity theft (IDT) to help prevent future IDT refund fraud.[8] The service on IRS's website allowed taxpayers to retrieve their IP PINs online by passing IRS's authentication checks. These checks confirm taxpayer identity by asking for personal, financial and tax-related information. The IRS stated that it was conducting further review of the IP PIN service and is looking at further strengthening the security features before resuming service. As of April 7, the online service was still suspended.

The Commissioner of Internal Revenue has overall responsibility for ensuring the confidentiality, integrity, and availability of the information and systems that support the agency and its operations. Within IRS, the senior agency official responsible for information security is the Associate CIO, who heads the IRS Information Technology Cybersecurity organization.

[8]In January 2014, IRS offered a limited IP PIN pilot program to eligible taxpayers in Florida, Georgia, and the District of Columbia. Taxpayers must confirm their identities with IRS to receive an IP PIN. IP PINs help prevent future IDT refund fraud because, once issued, the IP PIN must accompany their electronically filed tax return or else IRS will reject the return. If a paper return has a missing or incorrect IP PIN, IRS delays processing the return while the agency determines if it was filed by the legitimate taxpayer. See GAO, *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud*, GAO-14-633 (Washington, D.C.: Aug. 20, 2014), for more details on IRS's IP PIN service.

Although IRS Has Made Improvements, Information Security Weaknesses Continue to Place Taxpayer and Financial Data at Risk

As we reported in March 2016,[9] IRS has implemented numerous controls over key financial and tax processing systems; however, it had not always effectively implemented access and other controls,[10] including elements of its information security program.

Access controls are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. These controls include identification and authentication, authorization, cryptography, audit and monitoring, and physical security controls, among others. In our most recent review we found that IRS had improved access controls, but some weaknesses remain.

- **Identifying and authenticating** users—such as through user account-password combinations—provides the basis for establishing accountability and controlling access to a system. IRS established policies for identification and authentication, including requiring multifactor authentication[11] for local and network access accounts and establishing password complexity and expiration requirements. It also improved identification and authentication controls by, for example, expanding the use of an automated mechanism to centrally manage, apply, and verify password requirements. However, weaknesses in identification and authentication controls remained. For example, the agency used easily guessable passwords on servers supporting key systems.

[9]GAO, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, GAO-16-398 (Washington, D.C.: Mar. 28, 2016).

[10]Information security controls include logical and physical access controls, configuration management, and continuity of operations. These controls are designed to ensure that access to data is properly restricted, physical access to sensitive computing resources and facilities is protected, systems are securely configured to avoid exposure to known vulnerabilities, and backup and recovery plans are adequate and tested to ensure the continuity of essential operations.

[11]Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric).

- **Authorization controls** limit what actions users are able to perform after being allowed into a system and should be based on the concept of "least privilege," granting users the least amount of rights and privileges necessary to perform their duties. While IRS established policies for authorizing access to its systems, it continued to permit excessive access in some cases. For example, users were granted rights and permissions in excess of what they needed to perform their duties, including for an application used to process electronic tax payment information and a database on a human resources system.

- **Cryptography controls** protect sensitive data and computer programs by rendering data unintelligible to unauthorized users and protecting the integrity of transmitted or stored data. IRS policies require the use of encryption and it continued to expand its use of encryption to protect sensitive data. However, key systems we reviewed had not been configured to encrypt sensitive user authentication data.

- **Audit and monitoring** is the regular collection, review, and analysis of events on systems and networks in order to detect, respond to, and investigate unusual activity. IRS established policies and procedures for auditing and monitoring its systems and continued to enhance its capability by, for example, implementing an automated mechanism to log user activity on its access request and approval system. But it had not established logging for two key applications used to support the transfer of financial data and access and manage taxpayer accounts; nor was the agency consistently maintaining key system and application audit plans.

- **Physical security controls**, such as physical access cards, limit access to an organization's overall facility and areas housing sensitive IT components. IRS established policies for physically protecting its computer resources and physical security controls at its enterprise computer centers, such as a dedicated guard force at each of its computer centers. However, the agency had yet to address weaknesses in its review of access lists for both employees and visitors to sensitive areas.

IRS also had weaknesses in configuration management controls, which are intended to prevent unauthorized changes to information system resources (e.g., software and hardware) and provide assurance that systems are configured and operating securely. Specifically, while IRS developed policies for managing the configuration of its IT systems and improved some configuration management controls, it did not, for

example, ensure security patch updates were applied in a timely manner to databases supporting 2 key systems we reviewed, including a patch that had been available since August 2012.

To its credit, IRS had established contingency plans for the systems we reviewed, which help ensure that when unexpected events occur, critical operations can continue without interruption or can be promptly resumed, and that information resources are protected. Specifically, IRS had established policies for developing contingency plans for its information systems and for testing those plans, as well as for implementing and enforcing backup procedures. Moreover, the agency had documented and tested contingency plans for its systems and improved continuity of operations controls for several systems.

Nevertheless, the control weaknesses can be attributed in part to IRS's inconsistent implementation of elements of its agency-wide information security program. The agency established a comprehensive framework for its program, including assessing risk for its systems, developing system security plans, and providing employees with security awareness and specialized training. However, IRS had not updated key mainframe policies and procedures to address issues such as comprehensively auditing and monitoring access.

In addition, the agency had not fully addressed previously identified deficiencies or ensured that its corrective actions were effective. During our most recent review, IRS told us it had addressed 28 of our prior recommendations; however, we determined that 9 of these had not been effectively implemented.

The collective effect of the deficiencies in information security from prior years that continued to exist in fiscal year 2015, along with the new deficiencies we identified, are serious enough to merit the attention of those charged with governance of IRS and therefore represented a significant deficiency in IRS's internal control over financial reporting systems as of September 30, 2015.[12]

[12]A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit the attention of those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

Implementing GAO Recommendations Can Help IRS Better Protect Sensitive Taxpayer and Financial Data

To assist IRS in fully implementing its agency-wide information security program, we made two new recommendations to more effectively implement security-related policies and plans. In addition, to assist IRS in strengthening security controls over the financial and tax processing systems we reviewed, we made 43 technical recommendations in a separate report with limited distribution to address 26 new weaknesses in access controls and configuration management.[13]

Implementing these recommendations—in addition to the 49 outstanding recommendations from previous audits—will help IRS improve its controls for identifying and authenticating users, limiting users' access to the minimum necessary to perform their job-related functions, protecting sensitive data when they are stored or in transit, auditing and monitoring system activities, and physically securing its IT facilities and resources.

Table 1 below provides the number of our prior recommendations to IRS that were not implemented at the beginning of our fiscal year 2015 audit, how many were resolved by the end of the audit, new recommendations, and the total number of outstanding recommendations at the conclusion of the audit.

[13]GAO, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, GAO-16-397SU (Washington, D.C.: Mar. 28, 2016).

Table 1: Status of GAO's Information Security Recommendations at the Conclusion of Fiscal Year 2015 Audit

Control area	Prior recommendations not implemented at the beginning of fiscal year 2015 audit	Recommendations implemented or considered no longer relevant at the end of fiscal year 2015 audit	Prior recommendations not fully implemented at the end of fiscal year 2015 audit	New recommendations made during fiscal year 2015 audit	Total outstanding recommendations at the conclusion of fiscal year 2015 audit
Information security program	12	3	9	2	11
Access controls					
Identification and authentication	6	1	5	9	14
Authorization	10	4	6	12	18
Cryptography	8	3	5	14	19
Audit and monitoring	6	1	5	3	8
Physical Security	4	2	2	0	2
Other security controls					
Configuration management	21	5	16	5	21
Segregation of duties	1	0	1	0	1
Contingency planning	2	2	0	0	0
Total:	**70**	**21**	**49**	**45**	**94**

Source: GAO analysis of IRS data. | GAO-16-589T

In commenting on drafts of our reports presenting the results of our fiscal year 2015 audit, the IRS Commissioner stated that while the agency agreed with our new recommendations, it will review them to ensure that its actions include sustainable fixes that implement appropriate security controls balanced against IT and human capital resource limitations.

In addition, IRS can take steps to improve its response to data breaches. Specifically, in December 2013 we reported on the extent to which data breach policies at eight agencies, including IRS, adhered to requirements and guidance set forth by the Office of Management and Budget and the National Institute of Standards and Technology.[14] While the agencies in

[14]GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

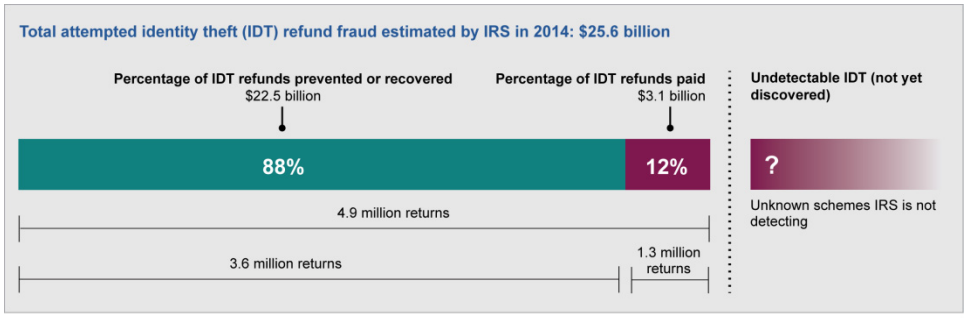
our review generally had policies and procedures in place that reflected the major elements of an effective data breach response program, implementation of these policies and procedures was not consistent. With respect to IRS, we determined that its policies and procedures generally reflected key practices, although the agency did not require considering the number of affected individuals as a factor when determining if affected individuals should be notified of a suspected breach. In addition, IRS did not document lessons learned from periodic analyses of its breach response efforts. We recommended that IRS correct these weaknesses, but the agency has yet to fully address them.

Billions of Dollars Have Been Lost to IDT Refund Fraud, and IRS Faces Challenges in Combating This Evolving Threat

The importance of protecting taxpayer information is further highlighted by the billions of dollars that have been lost to IDT refund fraud, which continues to be an evolving threat. IRS develops estimates of the extent of IDT refund fraud to help direct its efforts to identify and prevent the crime. While its estimates have inherent uncertainty, IRS estimated that it prevented or recovered $22.5 billion in fraudulent IDT refunds in filing season 2014 (see figure 1).[15] However, IRS also estimated, where data were available, that it paid $3.1 billion in fraudulent IDT refunds. Because of the difficulties in knowing the amount of undetectable fraud, the actual amount could differ from these estimates.

[15]IRS's 2014 estimates cannot be compared to 2013 estimates because of substantial methodology changes to better reflect new IDT refund fraud schemes and to improve the accuracy of its estimates, according to IRS officials. GAO is reviewing IRS's IDT refund fraud estimates as part of ongoing work.

Figure 1: IRS Estimates of Attempted Identity Theft Refund Fraud, 2014



Source: GAO analysis of IRS data. | GAO-16-589T

IRS has taken steps to address IDT refund fraud; however, it remains a persistent and continually changing threat. IRS recognized the challenge of IDT refund fraud in its fiscal year 2014-2017 strategic plan and increased resources dedicated to combating IDT and other types of refund fraud.[16] In fiscal year 2015, IRS reported that it staffed more than 4,000 full-time equivalents and spent about $470 million on all refund fraud and IDT activities.[17] As described above, IRS received an additional $290 million for fiscal year 2016 to improve customer service, IDT identification and prevention, and cybersecurity efforts and the agency plans to use $16.1 million of this funding to help prevent IDT refund fraud, among other things. The administration requested an additional $90 million and an additional 491 full-time equivalents for fiscal year 2017 to help prevent IDT refund fraud and reduce other improper payments.[18] IRS estimates that this $90 million investment in IDT refund fraud and other improper payment prevention would help it protect $612 million in revenue in fiscal year 2017, as well as protect revenue in future years.

IRS has taken action to improve customer service related to IDT refund fraud. For example, between the 2011 and 2015 filing seasons, IRS experienced a 430 percent increase in the number of telephone calls to its Identity Theft Toll Free Line—as of March 19, 2016, IRS had received

[16]IRS, *Strategic Plan*: FY2014-2017, (Washington, D.C.: June 2014).

[17]IRS officials told us they do not track spending for identity theft activities separately from other types of refund fraud. A full-time equivalent reflects the total number of regular straight-time hours (i.e., not including overtime or holiday hours) worked by employees divided by the number of compensable hours applicable to each fiscal year.

[18]Improper payments are payments that should not have been made or that were made in an incorrect amount (including overpayments and underpayments).

over 1.1 million calls to this line.[19] Moreover, 77 percent of callers seeking assistance on this telephone line received it compared to 54 percent during the same period last year. Average wait times during the same period have also decreased—taxpayers are waiting an average of 14 minutes to talk to an assistor, a decrease from 27 minutes last year.

IRS also works with third parties, such as tax preparation industry participants, states, and financial institutions to try to detect and prevent IDT refund fraud. In March 2015, the IRS Commissioner convened a Security Summit with industry and states to improve information sharing and authentication. IRS officials said that 40 state departments of revenue and 20 tax industry participants have officially signed a partnership agreement to enact recommendations developed and agreed to by summit participants. IRS plans to invest a portion of the $16.1 million it received in fiscal year 2016 into identity theft prevention and refund fraud mitigation actions from the Security Summit. These efforts include developing an Information Sharing and Analysis Center where IRS, states, and industry can share information to combat IDT refund fraud.

Even though IRS has prioritized combating IDT refund fraud, fraudsters adapt their schemes to identify weaknesses in IDT defenses, such as gaining access to taxpayers' tax return transcripts through IRS's online Get Transcript service.[20] According to IRS officials, with access to tax transcripts, fraudsters can create historically consistent returns that are hard to distinguish from a return filed by a legitimate taxpayer, potentially making it more difficult for IRS to identify and detect IDT refund fraud.

Implementing Past GAO Recommendations Could Help IRS Combat IDT Refund Fraud

Without additional action by IRS and Congress, the risk of issuing fraudulent IDT refunds could grow. We previously made recommendations to IRS to help it better combat IDT refund fraud:

- **Authentication**. In January 2015, we reported that IRS's authentication tools have limitations and recommended that IRS

[19]Total call volume to IRS's identity theft protection toll free telephone line includes automated and assistor calls answered, as well as those that received a busy signal or were abandoned or disconnected,

[20]As mentioned above, the online Get Transcript service has been unavailable since May 2015.

assess the costs, benefits and risks of its authentication tools.[21] For example, individuals can obtain an e-file PIN by providing their name, Social Security number, date of birth, address, and filing status for IRS's e-file PIN application. Identity thieves can easily find this information, allowing them to bypass some, if not all, of IRS's automatic checks, according to our analysis and interviews with tax software and return preparer associations and companies. After filing an IDT return using an e-file PIN, the fraudulent return would proceed through IRS's normal return processing.

In November 2015, IRS officials told us that the agency had developed guidance for its Identity Assurance Office to assess costs, benefits, and risk, and that its analysis will inform decision-making on authentication-related issues. IRS also noted that the methods of analysis for the authentication tools will vary depending on the different costs and other factors for authenticating taxpayers in different channels, such as online, phone, or in-person. In February 2016, IRS officials told us that the Identity Assurance Office plans to complete a strategic plan for taxpayer authentication across the agency in September 2016. While IRS is taking steps, it will still be vulnerable until it completes and uses the results of its analysis of costs, benefits, and risk to inform decision-making.

- **Form W-2, *Wage and Tax Statement* (W-2) Pre-refund Matching**. In August 2014 we reported that the wage information that employers report on Form W-2 is not available to IRS until after it issues most refunds, and that if IRS had access to W-2 data earlier, it could match such information to taxpayers' returns and identify discrepancies before issuing billions of dollars of fraudulent IDT refunds.[22] We recommended that IRS assess the costs and benefits of accelerating W-2 deadlines.

  In response to our recommendation, IRS provided us with a report in September 2015 discussing (1) adjustments to IRS systems and work processes needed to use accelerated W-2 information, (2) the potential impacts on internal and external stakeholders, and (3) other

[21]GAO, *Identity Theft and Tax Fraud: Enhanced Authentication Could Combat Refund Fraud but IRS Lacks an Estimate of Costs, Benefits and Risks*, GAO-15-119, (Washington, D.C.: Jan. 20, 2015).

[22]GAO, *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud*, GAO-14-633 (Washington, D.C.: Aug. 20, 2014).

changes needed to match W-2 data to tax returns prior to issuing refunds, such as delaying refunds until W-2 data are available. In December 2015, the Consolidated Appropriations Act of 2016 amended the tax code to accelerate W-2 filing deadlines to January 31.[23] IRS's report will help IRS determine how to best implement pre-refund W-2 matching, given the new January 31st deadline for filing W-2s. Additionally, we suggested that Congress should consider providing the Secretary of the Treasury with the regulatory authority to lower the threshold for electronic filing of W-2s, which could make more W-2 information available to IRS earlier.

- **External Leads**. IRS partners with financial institutions and other external parties to obtain information about emerging IDT refund trends and fraudulent returns that have passed through IRS detection systems. In August 2014, we reported that IRS provides limited feedback to external parties on IDT external leads they submit and offers external parties limited general information on IDT refund fraud trends and recommended that IRS provide actionable feedback to all lead generating third parties.[24]

  In November 2015, IRS reported that it had developed a database to track leads submitted by financial institutions and the results of those leads. IRS also stated that it had held two sessions with financial institutions to provide feedback on external leads provided to IRS. In December 2015, IRS officials stated that the agency sent a customer satisfaction survey asking financial institutions for feedback on the external leads process and was considering other ways to provide feedback to financial institutions. In April 2016, IRS officials stated they plan to analyze preliminary survey results by mid-April 2016. Additionally, IRS officials reported that the agency shared information with financial institutions in March 2016 and plans to do so on a quarterly basis, with the next information sharing session scheduled in June 2016.

[23]Pub. L. No. 114-113, div. Q, § 201, 129 Stat. 2242 (Dec. 18, 2015). This change goes into effect for W-2s reporting payments made in 2016 and filed in 2017.

[24]GAO-14-633.

The 2016 Filing Season Has Generally Been Smooth, and Telephone Service Has Improved

IRS and industry partners have characterized that returns processing and refund issuance during this filing season has been generally smooth. Through April 1, 2016, IRS had processed about 95 million returns and issued 76 million refunds totaling about $215 billion. While IRS experienced a major system failure in February that halted returns processing for about a day, the agency reported that it had minimal effect on overall processing of returns and refunds.

In addition to filing returns, many taxpayers often call IRS for assistance. IRS's telephone service has generally improved in 2016 over last year. From January 1 through March 19, 2016 IRS received about 35.4 million calls to its automated and live assistor telephone lines, about a 2 percent decrease compared to the same period last year.[25] Of the 13.4 million calls seeking live assistance, IRS had answered 9.1 million calls—a 75 percent increase over the 5.2 million calls answered during the same period last year.

IRS anticipated that 65 percent of callers seeking live assistance would receive it this filing season, which runs through April 18, and 47 percent of callers would receive live assistance through the entire 2016 fiscal year.[26] As of March 19, 2016, 75 percent of callers had received live assistance, an increase from 38 percent during the same period last year. Further, the average wait time to speak to an assistor also decreased from 24 to 9 minutes. As we reported in March 2016, however, IRS's telephone level of service for the full fiscal year has yet to reach the levels it had achieved in earlier years.[27]

IRS attributed this year's service improvement to a number of factors. Of the additional $290 million IRS received in December 2015, it allocated

[25]Total call volume to IRS's toll free telephone lines include automated and assistor calls answered, as well as those that received a busy signal or were abandoned or disconnected,

[26]This year, most taxpayers have until April 18 to file a tax return with IRS. IRS's projected telephone level of service for the filing season covers the period between January 1, 2016 and April 23, 2016.

[27]GAO, *Internal Revenue Service: Preliminary Observations on the Fiscal Year 2017 Budget Request and 2016 Filing Season Performance*, GAO-16-459R (Washington, D.C.: Mar. 8, 2016).

$178.4 million (61.5 percent) for taxpayer services to make measurable improvements in its telephone level of service. With the funds, IRS hired 1,000 assistors who began answering taxpayer calls in March, in addition to the approximately 2,000 seasonal assistors it had hired in fall 2015.[28] To help answer taxpayer calls before March, IRS officials told us that they detailed 275 staff from one of its compliance functions to answer telephone calls.[29] IRS officials said they believe this step was necessary because the additional funding came too late in the year to hire and train assistors to fully cover the filing season. IRS also plans to use about 600 full-time equivalents of overtime for assistors to answer telephone calls and respond to correspondence in fiscal year 2016, compared to fewer than 60 full-time equivalents of overtime used in fiscal year 2015.

In December 2014, we recommended that IRS systematically and periodically compare its telephone service to the best in business to identify gaps between actual and desired performance.[30] IRS disagreed with this recommendation, noting that it is difficult to identify comparable organizations. We do not agree with IRS's position; many organizations run call centers that would provide ample opportunities to benchmark IRS's performance.

In fall 2015, Department of the Treasury (Treasury) and IRS officials said they had no plans to develop a comprehensive customer service strategy or specific goals for telephone service tied to the best in the business and customer expectations. Without such a strategy, Treasury and IRS can neither measure nor effectively communicate to Congress the types and levels of customer service taxpayers should expect and the resources needed to reach those levels. Therefore, in December 2015 we suggested that Congress consider requiring that Treasury work with IRS to develop a comprehensive customer service strategy.[31] In April 2016, IRS officials told us that the agency established a team to consider our

[28]In contrast, IRS reduced the number of assistors answering telephone calls between fiscal years 2010 and 2015, which contributed to the lowest level of telephone service in fiscal year 2015 compared to recent years.

[29]IRS has not yet determined the amount of foregone revenue from taking this action.

[30]GAO, *Tax Filing Season: 2014 Performance Highlights the Need to Better Manage Taxpayer Service and Future Risks,* GAO-15-163 (Washington, D.C.: Dec. 16, 2014).

[31]GAO, *2015 Tax Filing Season: Deteriorating Taxpayer Service Underscores Need for a Comprehensive Strategy and Process Efficiencies,* GAO-16-151 (Washington, D.C.: Dec. 16, 2015).

prior work in developing this strategy or benchmarking its telephone service.

In summary, while IRS has made progress in implementing information security controls, it needs to continue to address weaknesses in access controls and configuration management and consistently implement all elements of its information security program. The risks IRS and the public are exposed to have been illustrated by recent incidents involving public-facing applications, highlighting the importance of securing systems that contain sensitive taxpayer and financial data. In addition, fully implementing key elements of a breach response program will help ensure that when breaches of sensitive data do occur, their impact on affected individuals will be minimized.

Weaknesses in information security can also increase the risk posed by identity theft refund fraud. IRS needs to establish an approach for addressing identity theft refund fraud that is informed by assessing the cost, benefits, and risks of IRS's various authentication options and improving the reliability of fraud estimates.

While this year's tax filing season has generally gone smoothly and IRS has improved customer service, it still needs to develop a comprehensive approach to customer service that will meet the needs of taxpayers while ensuring that their sensitive information is adequately protected.

Chairman Hatch, Ranking Member Wyden, and Members of the Committee, this concludes my statement. I look forward to answering any questions that you may have at this time.

Contacts and Staff Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, Nancy Kingsbury at (202) 512-2928 or kingsburyn@gao.gov, or James R. McTigue, Jr. at (202) 512-9110 or mctiguej@gao.gov or Jessica K. Lucas-Judy at (202) 512-9110 or LucasJudyJ@gao.gov. Other key contributors to this statement include Jeffrey Knott, Neil A. Pinney, and Joanna M. Stamatiades (assistant directors); Dawn E. Bidne; Mark Canter; James Cook; Shannon J. Finnegan; Lee McCracken; Justin Palk; J. Daniel Paulk; Erin Saunders Rath; and Daniel Swartz.