United States Government Accountability Office

Testimony

Before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, April 14, 2016

INFORMATION SECURITY

IRS Needs to Further Enhance Controls over Taxpayer and Financial Data

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-16-590T

April 14, 2016

INFORMATION SECURITY

IRS Needs to Further Enhance Controls over Taxpayer and Financial Data

GAO Highlights

Highlights of GAO-16-590T, a testimony before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives

Why GAO Did This Study

In collecting taxes, processing returns, and providing taxpayer service, IRS relies extensively on computerized information systems. Accordingly, 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 that occurs when a thief files a fraudulent tax return using a legitimate taxpayer's identity and claims a refund.

Since 1997, GAO has designated federal information security as a government-wide high-risk area, and in 2015 it expanded this area to include the protection of personally identifiable information. GAO also added identity theft refund fraud to its high-risk area on the enforcement of tax laws.

This statement discusses (1) IRS's information security controls over tax processing and financial systems and (2) roles that federal agencies with government-wide information security responsibilities play in providing guidance and oversight to agencies. This statement is based on previously published GAO work and a review of federal guidance.

What GAO Recommends

In addition to 49 prior recommendations that had not been implemented, GAO made 45 new recommendations to IRS in March 2016 to further improve its information security controls and program. GAO also recommended that IRS assess costs, benefits, and risks of taxpayer authentication options.

View GAO-16-590T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or James R. McTigue, Jr. at (202) 512-9110 or mctiguej@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 safeguards intended to properly restrict access to systems and information. In particular, while IRS had improved some of its access controls, weaknesses remained with identifying and authenticating users, authorizing users' level of rights and privileges, encrypting sensitive data, auditing and monitoring network activity, and physically securing its computing resources. These weaknesses were due in part to IRS's inconsistent implementation of its agency-wide security program, including not fully implementing GAO recommendations. The table below shows the status of prior and new GAO recommendations as of the end of its fiscal year (FY) 2015 audit of IRS's information security. GAO concluded that these weaknesses collectively constituted a significant deficiency for the purposes of financial reporting for fiscal year 2015. Until they are effectively mitigated, taxpayer and financial data will continue to be exposed to unnecessary risk.

Status of GAO Information Security Recommendations to IRS as of March 2016

Information security control area	Prior GAO recommendations open at the start of FY 2015 audit	Recommendations closed during FY 2015 audit	New recommendations	Outstanding recommendations at end of FY 2015 audit
Information security program	12	(3)	2	11
Access controls	34	(11)	38	61
Other controls	24	(7)	5	22
Totals	70	(21)	45	94

Source: GAO analysis of IRS data. | GAO-16-590T

The importance of protecting taxpayer information is further highlighted by the billions of dollars that have been lost to identity theft refund fraud, which continues to be an evolving threat. While IRS has taken steps to address this issue, as GAO reported in January 2015 it has yet to assess the costs, benefits, and risks of methods for improving the authentication of taxpayers' identity.

The Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) provide government-wide guidance and oversight for federal information security. These agencies have taken a number of actions to carry out these responsibilities. For example:

- OMB has prescribed security policies, including direction on ensuring that online services provided by agencies are secure and protect privacy.
- NIST has developed standards and guidelines for implementing security controls, including those for authenticating users during online transactions.
- DHS has issued a directive requiring departments and agencies to mitigate critical vulnerabilities on their Internet-facing systems. It also assists agencies in monitoring their networks for malicious traffic.

Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's timely hearing on information security at the Internal Revenue Service (IRS). As taxpayers file their returns for 2015, it is especially important that 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.

As requested, my statement today will discuss (1) information security controls over tax processing and financial systems at IRS and (2) roles that federal agencies with government-wide information security responsibilities play in providing guidance and oversight to executive branch agencies. In preparing this statement, we relied on previously published work on IRS and government-wide information security. We also reviewed relevant federal laws and information security-related guidance issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). The GAO reports cited in this statement each contain a detailed description of the scope of

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

the work on which they are based and the methodologies used to carry it out.

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

Background

As technology has advanced, the federal government has become increasingly dependent on computerized information systems to carry out operations and process, maintain, and report essential information. Federal agencies rely on such systems to process, maintain, and report large volumes of sensitive data, such as personal information.

Ineffective protection of these systems and information can impair delivery of vital services and result in

- loss or theft of computer resources, assets, and funds;
- inappropriate access to and disclosure, modification, or destruction of sensitive information, such as PII;
- undermining of agency missions due to embarrassing incidents that erode the public's confidence in government;
- damage to networks and equipment; and
- high costs for remediation.

Recognizing the importance of these issues, federal law includes requirements intended to improve the protection of government information and systems. These laws include the Federal Information Security Modernization Act (FISMA) of 2014, which 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.[3]

More specifically, federal agencies are to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the operations of the agency, including those provided or managed by another agency, a contractor, or other organization on behalf of the agency. In addition, the head of each agency is responsible for, among other things, ensuring that senior agency officials carry out their information security responsibilities and that all personnel are held accountable for complying with the agency-wide information security program.

The act also assigned OMB and the Department of Homeland Security (DHS) oversight responsibilities to assist agencies in effectively implementing information security protections. In addition, NIST is responsible for developing standards and guidelines that include minimum information security requirements.

IRS Relies on Information Technology Systems to Carry out Its Role as Tax Collector for the United States

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. 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.

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

[3]The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014)) partially superseded the Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this statement, "FISMA" refers to the new requirements in FISMA 2014, FISMA 2002 requirements relevant here that were incorporated and continued in FISMA 2014, and other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

U.S. embassies and consulates. To manage its data and information, the agency operates two enterprise computing centers. It also collects and maintains a significant amount of personal and financial information on each U.S. taxpayer. Protecting this sensitive information is essential to protecting taxpayers' privacy and preventing financial loss and damages that could result from identity theft and other financial crimes. Further, the size and complexity of the IRS add unique operational challenges.

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.

Cyber Threats Facing Federal Systems Continue to Evolve

Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused by natural disasters, defective computer or network equipment, software coding errors, and the actions of careless or poorly trained employees. Intentional threats include targeted and untargeted attacks from criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists. These adversaries vary in terms of their capabilities, willingness to act, and motives.

These threat sources make use of various techniques—or exploits—that may adversely affect federal information, computers, software, networks, and operations. These exploits are carried out through various conduits, including websites, e-mails, wireless and cellular communications, Internet protocols, portable media, and social media. Further, adversaries can leverage common computer software programs as a means by which to deliver a threat by embedding exploits within software files that can be activated when a user opens a file within its corresponding program.

The number of information security incidents affecting systems supporting the federal government is increasing. Specifically, the number of incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) increased from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent. This upward trend continues. According to OMB, agencies reported 77,183 incidents in fiscal year 2015. Similarly, the number of incidents involving PII reported by federal agencies has more than doubled in recent years, from 10,481 in 2009 to 27,624 in 2014.

Moreover, for fiscal year 2015, OMB reported that federal agencies spent about $13.1 billion on cybersecurity,[4] and agencies budgeted about $14 billion for cybersecurity for fiscal year 2016.[5] This amount may increase significantly, as the president's fiscal year 2017 budget proposes investing over $19 billion in resources for cybersecurity.

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.[6] According to officials, criminals used taxpayer-specific data acquired from non-agency 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 reported 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

[4]OMB, *Annual Report to Congress: Federal Information Security Modernization Act*, (Washington, D.C.: Mar. 18, 2016).

[5]OMB, *Middle Class Economics: Cybersecurity*, The President's Budget Fiscal Year 2016 (Washington, D.C.: Feb. 2, 2015).

[6]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.

of identity theft (IDT) to help prevent future IDT refund fraud.[7] 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. As of April 7, the online service was still suspended.

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

As we reported in March 2016, IRS has implemented numerous protections over key financial and tax processing systems; however, it had not always effectively implemented access and other controls, including elements of its information security program.[8]

Access controls are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. They include identification and authentication, authorization, cryptography, audit and monitoring, and physical security, among others. In our most recent review we determined 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

[7]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 identity theft refund fraud (discussed later in this statement) 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.

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

multifactor authentication[9] 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. In addition, while IRS continued to expand the use of two-factor access to its network, the Treasury Inspector General for Tax Administration reported that IRS had not fully implemented unique user identification and authentication or remote electronic authentication that complies with federal requirements.[10]

- **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 the agency 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.

[9]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).

[10]Treasure Inspector General for Tax Administration, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2015*, 2015-20-092 (Sept. 25, 2015). Homeland Security Presidential Directive 12, issued in August 2004, directed the establishment of a mandatory government-wide standard for secure and reliable forms of identification for federal employees and contractor personnel who access government-controlled facilities and information systems.

- **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 two 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 mitigated previously identified deficiencies or ensured that its corrective actions were effective. During our most recent review, IRS told us it had completed corrective actions for 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.[11]

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.[12]

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

[11]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.

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

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.

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-16-590T

In commenting on drafts of the 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.

We have also previously reported that IRS can take steps to improve its response to data breaches involving the inappropriate disclosure—or potential disclosure—of personally identifiable information. 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 OMB and NIST.[13] While the agencies in 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.

IRS Faces Challenges in Addressing Identity Theft Refund Fraud

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. IDT refund fraud 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. This crime burdens legitimate taxpayers because authenticating their identities is likely to delay the processing of their tax 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 our high-risk area on the enforcement of tax laws to include IRS's efforts to address IDT refund fraud.[14]

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. However, it also estimated that it paid $3.1 billion in fraudulent IDT refunds.

[13]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).

[14]GAO-15-290.

IRS has taken steps to address IDT refund fraud; however, it remains a persistent and evolving threat. For example in its fiscal year 2014-2017 strategic plan, IRS increased resources dedicated to combating IDT and other types of refund fraud. In 2015, IRS reported allocating more than 4,000 full-time equivalent staff and spending $470 million on refund fraud and IDT activities. In addition, IRS received an additional $290 million for fiscal year 2016 to improve customer service, IDT identification and prevention, and cybersecurity efforts.

The agency has also taken actions to improve customer service related to IDT fraud by, for example, providing an increased level of service to taxpayers calling its identity theft toll-free phone line. In addition, IRS has worked with tax preparation professionals, states, and financial institutions to better detect and prevent IDT fraud.

These efforts notwithstanding, fraudsters continue to adapt their schemes to identify weaknesses in IDT defense, such as by gaining access to taxpayers' tax return transcripts through IRS's online Get Transcript service. According to IRS officials, this allows fraudsters to create historically consistent returns that are hard to distinguish from one filed by a legitimate taxpayer.

These continuing challenges highlight the need for additional actions by IRS. As we have reported, there are steps IRS can take to, among other things, better authenticate the identity of taxpayers before issuing refunds. In January 2015 we reported that IRS's authentication tools have limitations.[15] For example, individuals could 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. After filing an IDT return using an e-file PIN, the fraudster could file a fraudulent return through IRS's normal return processing. Accordingly, we recommended that IRS assess the costs, benefits, and risks of its authentication options.

In November 2015, IRS officials told us that the agency had developed guidance for its Identity Assurance Office to assess costs, benefits, and risk of authentication tools. In February 2016, officials told us that this office plans to complete a strategic plan for taxpayer authentication across the agency in September 2016. Until it completes these steps, IRS

[15]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).

will lack key information to make decisions about whether and how much to invest in authentication options.

Agencies with Government-Wide Responsibilities Play a Key Role in Guiding and Overseeing Federal Information Security

Under FISMA, the Director of OMB is responsible for developing and overseeing the implementation of policies, principles, standards, and guidelines on information security in federal agencies, except with regard to national security and certain other systems. The director is also responsible for coordinating the development of standards and guidelines by NIST.

For its part, NIST is responsible under FISMA for developing security standards and guidelines for agencies that include standards for categorizing information and information systems according to ranges of impact levels, minimum security requirements for information and information systems in risk categories, guidelines for detection and handling of information security incidents, and guidelines for identifying an information system as a national security system.

Accordingly, OMB and NIST have prescribed policies, standards, and guidelines that are intended to assist federal agencies with identifying and providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, alteration, and destruction of information and information systems, including those systems operated by a contractor or others on behalf of the agency. These include the following:

- OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*, which provides agencies with direction for managing information security risk on a continuous basis, including requirements for establishing information security continuous monitoring programs.

- NIST, Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.

- NIST Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information*

Systems, specifies minimum security requirements for federal agency information and information systems and a risk-based process for selecting the security controls necessary to satisfy these requirements.

- NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls.

OMB and NIST also have provided guidance to agencies on procedures for authenticating users to federal systems and websites, including the following:

- OMB M-15-13, *Policy to Require Secure Connections across Federal Websites and Web Services*, which requires all publicly accessible federal websites and web services to provide service through a secure connection.

- OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, which addresses federal government services accomplished using the Internet, instead of on paper, and calls for identity verification or authentication to make sure that online government services are secure and protect privacy. This guidance established four levels of identity assurance for electronic transactions requiring authentication. Each level describes the agency's degree of certainty that a user has presented an identifier that refers to his or her identity:
  - Level 1: little or no confidence in the asserted identity's validity.
  - Level 2: some confidence in the asserted identity's validity.
  - Level 3: high confidence in the asserted identity's validity.
  - Level 4: very high confidence in the asserted identity's validity.

- NIST Special Publication 800-63-2, *Electronic Authentication Guideline*, provides technical guidelines for federal agencies implementing electronic authentication and covers remote authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. Specifically, it provides technical requirements for agencies to use in selecting technology to achieve specified levels of e-authentication assurance, as defined by OMB and illustrated by the following examples:

- Level 1: Identity proofing[18] is not required. Successful authentication occurs when an individual proves through the means of authentication that he or she possesses and controls the token.[19] The cryptographic methods used at this level may still allow someone with malicious intent to intercept the transmission of a password through eavesdropping and crack it using a dictionary attack (i.e., guessing a password through trial-and-error using a dictionary).

- Level 2: Requires single-factor remote authentication, using one of three factors—something you know (e.g., a password), something you have (e.g., an identification badge), or something you are (e.g., a fingerprint). Identity proofing requirements are introduced, requiring presentation of identifying materials or information. Approved cryptographic methods would not allow the type of eavesdropping attack that is possible at Level 1.

- Level 3: Requires multi-factor remote authentication, requiring at least two authentication factors. An individual proves possession of a physical or software token in combination with some memorized knowledge. Approved cryptographic methods should be strong enough to protect against impersonation of the verifying entity.

- Level 4: Is intended to provide the highest practical remote network authentication assurance, requiring the proof of possession of a key through a cryptographic protocol. At this level in-person identity proofing is required. It is otherwise similar to Level 3, except with stronger cryptographic methods in place.

OMB and DHS Are Responsible for Oversight of Operational Aspects of Federal Cybersecurity

Federal law also gives OMB and DHS responsibility and authority for oversight of operational aspects of federal information security. In

[18]Identity proofing is the process of verifying information about an individual for the purposes of issuing credentials to that individual.

[19]According to NIST, a token is something that an individual possesses and controls (typically a cryptographic module or password) that is used to authenticate the individual's identity.

particular, the OMB Director is charged with overseeing and enforcing agency compliance with information security requirements by taking certain actions authorized by relevant federal law (discussed in more detail below), and OMB has developed various mechanisms to carry out its oversight function.

- **Budgetary authority:** Federal law gives OMB the power of enforcement and accountability related to evaluating agencies' management of their information resources, which includes ensuring that information security policies, procedures, and practices are adequate.[20] In particular, in enforcing accountability, OMB is empowered to recommend reductions or increases in an agency's budget and restrict the availability of funds for information resources, among other things.

- **OMB Cyber Unit:** In fiscal year 2015, OMB established the OMB Cyber and National Security Unit (OMB Cyber) within the Office of the Federal Chief Information Officer. This unit is responsible for strengthening federal cybersecurity through oversight of agency and government-wide programs, issuing and implementing policies to address emerging IT security risks, and oversight of government-wide response to major incidents and vulnerabilities.

- **CyberStat Reviews:** OMB has also established the "CyberStat Review" process, which involves evidence-based meetings led by OMB to ensure agencies are accountable for their cybersecurity posture, while assisting them in developing targeted, tactical actions to deliver results.

- **FISMA reporting:** As required by FISMA, OMB reports annually to Congress on the effectiveness of information security policies and practices at executive branch agencies during the preceding year and a summary of evaluations conducted by agency inspectors general.

Regarding DHS, the Federal Information Security Modernization Act of 2014 codified its responsibility for certain operational aspects of federal agency cybersecurity. In particular, DHS is responsible for

- administering, in consultation with OMB, the implementation of agency information security policies and practices for information

[20]40 U.S.C. § 11303(b)(5).

systems (other than national security systems, Department of Defense, and the intelligence community's "debilitating impact" systems);

- developing, issuing, and overseeing the implementation of binding operational directives to agencies on matters such as incident reporting, contents of agency's annual reports, and other operational requirements; and

- operating the federal information security incident center (the U.S Computer Emergency Readiness Team or US-CERT), deploying technology to continuously diagnose and mitigate threats, compiling and analyzing data, and developing and conducting targeted operational evaluations, including threat and vulnerability assessments of systems.

In May 2015 DHS issued its first directive, which required all departments and agencies to review and mitigate all critical vulnerabilities on their Internet-facing systems. DHS identifies these vulnerabilities using scanning tools and reports the results to agencies on a weekly basis. Agencies are then required to mitigate the DHS-identified vulnerabilities within 30 days of the report, or provide a justification to DHS outlining barriers, planned steps for resolution, and a time frame for mitigation.

DHS has also supplied agencies with tools and technologies to assist in protecting against cyber threats and vulnerabilities. For example:

- **Continuous Diagnostics and Mitigation Program:** Since fiscal year 2013, DHS has provided agencies the opportunity to use a suite tools and capabilities to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

- **National Cybersecurity Protection System:** NCPS is an integrated system-of-systems intended to deliver a range of capabilities for intrusion detection, intrusion prevention, analytics, and information sharing. When deployed on an agency's connection to the Internet, the system monitors inbound and outbound traffic for malicious activity.

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 is 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. IRS also needs to assess the costs, benefits, and risks of alternatives for better authenticating taxpayers who access its systems. Finally, strengthening the security posture of IRS—and other agencies—also depends on the key roles played by OMB, NIST, and DHS in providing oversight and guidance from a government-wide perspective, such as that related to improving authentication.

Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittee, this concludes my statement. I would be happy to answer any questions you have.

Contacts and 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. Other key contributors to this statement include Jeffrey L. Knott, Larry Crosland, John de Ferrari, and Neil A. Pinney (assistant directors); Dawn E. Bidne; Mark Canter; James Cook, Shannon J. Finnegan; Lee McCracken; Justin Palk; J. Daniel Paulk; Monica Perez-Nelson; David Plocher; Erin Saunders Rath; and Daniel Swartz.

Biography

Gregory Wilshusen is Director of Information Security Issues at GAO, where he leads cybersecurity and privacy-related studies and audits of the federal government and critical infrastructure. He has over 30 years of auditing, financial management, and information systems experience. Prior to joining GAO in 1997, Mr. Wilshusen held a variety of public and private sector positions. He was a senior systems analyst at the Department of Education. He also served as the Controller for the North Carolina Department of Environment, Health, and Natural Resources, and held senior auditing positions at Irving Burton Associates, Inc. and the U.S. Army Audit Agency. He's a certified public accountant, certified internal auditor, and certified information systems auditor. He holds a B.S. degree in business administration (accounting) from the University of Missouri and an M.S. in information management from George Washington University's School of Engineering and Applied Sciences.