Cybersecurity Act of 2015: Report on the Information Security Management Practices of the Internal Revenue Service

August 30, 2016

Reference Number: 2016-2R-079

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:
2 = Risk Circumvention of Agency Regulation or Statute

.

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

CYBERSECURITY ACT OF 2015: REPORT ON THE INFORMATION SECURITY MANAGEMENT PRACTICES OF THE INTERNAL REVENUE SERVICE

Highlights

Final Report issued on August 30, 2016

Highlights of Reference Number: 2016-2R-079 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As custodians of taxpayer information, the IRS has an obligation to protect this sensitive information against unauthorized access or loss in accordance with Federal requirements.

WHY TIGTA DID THE AUDIT

This audit was initiated to address the Cybersecurity Act of 2015, which mandated Inspectors General to submit a report to the committees of jurisdiction in the Senate and the House of Representatives on specific information security management practices of their respective agency, including logical access controls for unprivileged and privileged users, software license management, data exfiltration controls, and whether contractors also implemented these controls.

WHAT TIGTA FOUND

The IRS has established policy and practices for implementing the use of Personal Identity Verification (PIV) cards for its employees and contractors, as mandated by the August 2004 Homeland Security Presidential Directive 12. The IRS met the Fiscal Year 2016 cross-agency priority goal by requiring 85 percent or greater of people with unprivileged network accounts to log on with PIV cards, achieving 92 percent as of June 29, 2016. Also, 98 percent of the people with remote access were required to log on to the IRS's remote access solution using PIV cards as of June 29, 2016. In addition, the IRS reported that it met the cross-agency priority goal of 100 percent for people with privileged accounts required to log on with PIV cards, based on all privileged users being required to use PIV cards for general network access. Work is ongoing to ensure privileged access to systems using PIV cards. The IRS reported that eight of 140 systems are configured to support the use of PIV cards for access.

The IRS has established policies for conducting inventories of the software present on its systems and the licenses associated with the software, but it has not fully implemented these management practices. Although the IRS has various tools for managing its large inventory of hardware and software products, none are implemented enterprise-wide. Also, the IRS has not yet incorporated software license management into its software management program.

The IRS has implemented capabilities to monitor and detect exfiltration, with the exception of capabilities for digital rights management. The IRS has also implemented a data loss prevention solution to monitor outbound e-mail and web transmissions. The IRS's Computer Security Incident Response Center provides various capabilities that offer forensics and visibility. Also, following the Get Transcript application incident in Fiscal Year 2015, the IRS has taken steps to strengthen its network monitoring abilities.

The IRS requires contractors that provide services to the IRS using IRS-owned equipment to adhere to the level of controls specified for Federal agencies. For contractors that handle or manage IRS sensitive information using their own systems, the IRS issued Publication 4812, *Contractor Security Controls,* which contains a subset of Federal controls for moderate-impact systems. This subset includes comparable, but not always identical, controls for access, software and licensing inventories, and network monitoring. Federal guidance provides for agencies to consider such risk factors when determining baseline security controls for the external entities that handle Federal agency data.

WHAT TIGTA RECOMMENDED

TIGTA made no recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 30, 2016

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Cybersecurity Act of 2015: Report on the Information Security Management Practices of the Internal Revenue Service (Audit # 2016N11.CR03)

Title IV of the Cybersecurity Act of 2015,[1] Section 406, *Federal Computer Security*, mandated Inspectors General to submit a report to the committees of jurisdiction in the Senate and the House of Representatives on specific information security management practices. This report provides the Treasury Inspector General for Tax Administration's response regarding the specific information security management practices at the Internal Revenue Service.

Although we made no recommendations in this report, Internal Revenue Service officials were provided an opportunity to review the draft report; they did not provide any comments in response to this report.

If you have any questions, please contact me or Danny Verneuille, acting Assistant Inspector General for Audit (Security and Information Technology Services).

[1] Pub. L. No. I 14-1 13, Division N, § 406 (2015).

Table of Contents

Background ..... Page 1

Results of Review ..... Page 3

- Logical Access Policies and Practices Used to Access Covered Systems ..... Page 3
- Logical Access Controls and Multifactor Authentication Used to Control Access to Covered Systems by Privileged Users ..... Page 4
- Policies and Procedures for Conducting Inventories of the Software Present on Covered Systems and the Licenses Associated With the Software ..... Page 5
- Capabilities Used to Monitor and Detect Exfiltration and Other Threats ..... Page 6
- Policies and Procedures With Respect to Ensuring That Entities, Including Contractors, That Provide Services to the IRS Are Implementing the Above-Mentioned Information Security Management Practices ..... Page 9

Appendices

- Appendix I – Detailed Objective, Scope, and Methodology ..... Page 11
- Appendix II – Major Contributors to This Report ..... Page 13
- Appendix III – Report Distribution List ..... Page 14
- Appendix IV – Glossary of Terms ..... Page 15

Abbreviations

CSIRC	Computer Security Incident Response Center
FISMA	Federal Information Security Modernization Act
HSPD-12	Homeland Security Presidential Directive 12
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
PIV	Personal Identity Verification
SP	Special Publication
TIGTA	Treasury Inspector General for Tax Administration
U.S.C.	United States Code

Background

On December 18, 2015, the President signed into law the $1.1 trillion Omnibus Spending Bill that contained the Cybersecurity Act of 2015.[1] Title IV of this Act, Section 406, *Federal Computer Security*, contains a mandate for Inspectors General to report to the Senate and the House of Representatives Committees of jurisdiction on their agencies' policies and practices regarding "covered systems," including Federal computer systems providing access to Personally Identifiable Information or national security systems (as defined at 40 United States Code (U.S.C.) Section (§) 11103).

The Cybersecurity Act of 2015 requires Inspectors General to report on their agencies' information security policies and practices regarding Federal computer systems providing access to Personally Identifiable Information.

The report must be completed within 240 days of the enactment of the Act and include:

- A description of the logical access policies and practices used by the agency to control access to a covered system, including whether the appropriate standards were followed.
- A description and list of logical access controls and multifactor authentication used by the agency to control access to covered systems by privileged users. If the agency does not use such controls, then a description of why not.
- A description of the policies and procedures used to conduct inventories of the software present on covered systems and the licenses associated with such software.
- A description of the capabilities used to monitor and detect exfiltration and other threats, including:
    - Data loss prevention capabilities.
    - Forensics and visibility capabilities.
    - Digital rights management.

  If the agency is not using such capabilities, the report must include a description of why not.
- A description of the policies and procedures used to ensure entities, including contractors, that provide services to the agency are implementing the information security management practices mentioned above.

[1] Pub. L. No. I 14-1 13, Division N, § 406 (2015).

The Internal Revenue Service (IRS) collects and maintains a significant amount of personal and financial information on each taxpayer. As custodians of taxpayer information, the IRS has an obligation to protect this sensitive information against unauthorized access or loss in accordance with Federal requirements.

This report provides the Treasury Inspector General for Tax Administration's (TIGTA) response to the items above regarding specific information security management practices at the IRS. In addition to the most current information from the IRS, we also included relevant audit work from TIGTA where applicable.

This review was performed using information obtained from the IRS's Information Technology organization's Cybersecurity function in Lanham, Maryland, during the period May through August 2016. The scope of this review was to provide the cybersecurity information requested in the Cybersecurity Act of 2015. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Logical Access Policies and Practices Used to Access Covered Systems

The IRS has established policy and practices for implementing use of the Personal Identity Verification (PIV) card as the standard identity credential for its employees and contractors, as mandated by Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, signed by President Bush on August 27, 2004. The Administration has set certain high-priority metrics, called cybersecurity cross-agency priority goals, to measure Federal agencies' success in improving the security of their information operations. These goals include metrics for implementing PIV cards. For Fiscal Year 2016, the cybersecurity cross-agency priority goal for requiring people with unprivileged network accounts to log on with PIV cards is 85 percent or greater.

The IRS met this goal. As of June 29, 2016, 92 percent of people with unprivileged network accounts were required to access the network with PIV cards. The IRS indicated that the 8 percent who are not yet compliant are mainly due to tools or applications in use that are not compatible with PIV cards (5 percent) or seasonal workers who will not be issued PIV cards (2 percent). It is IRS policy not to issue cards to seasonal workers or other employees not expected to be employed at the IRS for more than 180 days. From the IRS HSPD-12 Weekly Reports that track estimated progress of PIV card implementation, as of June 29, 2016, the IRS had 80,621 individuals with unprivileged network accounts.

- 74,515 individuals (92.4 percent) with unprivileged network accounts who are required to log on with PIV cards.
- 4,379 individuals (5.4 percent) with unprivileged network accounts who are not required to log on with PIV cards.
- 1,727 individuals (2.1 percent) with unprivileged network accounts to whom PIV cards will not be issued.

The IRS HSPD-12 Weekly Reports also track PIV card implementation for remote access, which is the ability to access the IRS's nonpublic computing resources from locations external to IRS facilities. As of June 29, 2016, the IRS had 42,089 individuals with remote access to the IRS network, resources, or services.

- 41,187 individuals (98 percent) with remote access who are required to log on to the IRS's remote access solution with PIV cards.

- 198 individuals (0.5 percent) with remote access who are not required to log on to the IRS's remote access solution with PIV cards, but are required to log on with a non-PIV card form of two-factor authentication; that is, with use of a grid card.[2]
- 704 individuals (2 percent) with remote access who do not have PIV cards.

Lastly, the IRS captured metrics on the use of PIV cards to access its internal systems, including those Federal Information Security Modernization Act (FISMA)[3] systems owned and managed by the IRS that are accessed by internal organization users, defined as Federal employees, contractors, and affiliates. The IRS reported that it has 140 internal information systems that it manages. Of this number, the IRS further reported that eight internal systems are configured to support the use of PIV cards for access.

Logical Access Controls and Multifactor Authentication Used to Control Access to Covered Systems by Privileged Users

The IRS has also established policy and practices for implementing use of the PIV card for accessing covered systems by its privileged users. For Fiscal Year 2016, the cybersecurity cross-agency priority goal for requiring people with privileged network accounts to log on with PIV cards is 100 percent.

The IRS reported that it met this goal. The IRS asserts that all privileged users are first required to use their PIV card for general network access prior to using their privileged accounts, thereby meeting the definition of PIV-required for privileged users. The IRS indicated that use of this definition is consistent with the other Department of the Treasury bureaus. Following PIV-card access to the network, the privileged user may then need to access a legacy system that does not support PIV card access by using a user name and password. The IRS indicated that work is ongoing to ensure privileged access to systems using PIV cards and to replace aging systems and retire software that do not support PIV card access. As of June 29, 2016, the IRS had enabled a privileged access solution that allowed 1,901 (62 percent) of 3,084 privileged users to log on to privileged accounts using PIV cards.

The requirement that individuals needing privileged access to Federal networks and applications with a single PIV card and Personal Identification Number created a technological challenge across the Federal Government for an individual who needs both administrative and nonadministrative access to networks and information systems. The IRS has implemented a certificate mapping solution for privileged user authentication using PIV cards. This solution

[2] A grid card, or grid authentication, is a method of securing user logons by requiring the user to enter values from specific cells in a grid whose content should be only accessible to him and the service provider. Because the grid consists of letters and numbers in rows and columns, the method is sometimes referred to as bingo card authentication.

[3] Pub. L. No. 113-283. This bill amends chapter 35 of Title 44 of the U.S.C. to provide for reform to Federal information security.

populates the altSecurityID attribute from the PIV card to the IRS Active Directory and allows privileged users with a secondary administrator account to authenticate using their PIV card.

However, there are older technologies in use that do not support authentication using the PIV card. The IRS is in the process of retiring older versions of software and operating systems that do not support the use of the PIV card. In addition, the IRS is deploying new technology that will enhance security for situations in which it is unavoidable to use a password. In these situations, privileged users will be required to use a PIV card to request access to a system using a password. This will be accomplished using software the IRS has purchased (*i.e.*, the Total Privileged Access Manager from Dell) that is a multiplatform solution for privileged user access. The IRS indicated that this technology is needed to fully meet HSPD-12 requirements for privileged user access and that its implementation is planned for late summer 2016.

Policies and Procedures for Conducting Inventories of the Software Present on Covered Systems and the Licenses Associated With the Software

The IRS has established policies for conducting inventories of the software present on covered systems and the licenses associated with the software. In Fiscal Year 2013, the IRS also established the Enterprise Software Governance Board as a manual process to govern IRS enterprise software assets acquired from vendors (both commercial off-the-shelf and vendor-supported open source) throughout their lifecycle. The Board's responsibilities include tracking the use of software and its associated documentation and ensuring that the software is used in accordance with contract agreements, copyright laws, and licenses.

However, the IRS is still in the process of developing processes that rely on tools to manage its large inventory of hardware and software products, including licenses associated with the software. Although the IRS has various tools for managing its large inventory of hardware and software products, none are implemented enterprise-wide. Also, the IRS has not yet incorporated software license management into its software management program. The IRS is working to complete a number of software management actions, including developing an enterprise-wide repeatable method to manage and track the deployment of licenses that can uniformly be used by all IRS organizations responsible for managing licenses.

The IRS has implemented an asset management solution as its official inventory solution. However, the IRS's current asset discovery tool used to detect hardware and software in its environment does not integrate with its asset management inventory solution. As a result, the IRS is in the process of replacing its asset discovery tool with one that will integrate with its inventory solution.

Currently, the IRS maintains an authoritative inventory of its FISMA-reportable general support systems, major applications, and minor applications in the Treasury-owned tool called the Treasury FISMA Inventory Management System. The inventory tracks the manufacturer, model

number, serial number, Internet Protocol address, IRS barcode, hostname, function, software license number, interconnections, system/component information, and system/component owner. The IRS also manually tracks inventory components of its general support systems through Excel spreadsheets. Also, applications manage their specific inventories through their application-level Information Security Contingency Plan, which documents the hardware and software in use by the application.

Within the last three years, TIGTA completed three audits relating to software license management[4] and reported that the IRS was not adequately performing software license management, was not adhering to Federal requirements, and did not have specialized software license tools for developing and maintaining an enterprise-wide inventory. In addition, TIGTA reported in excess of $118 million in over- or under-deployment of software licenses. TIGTA is planning a follow-up audit in Fiscal Year 2017 to determine whether the IRS has made improvements in management of software licenses.

Capabilities Used to Monitor and Detect Exfiltration and Other Threats

The IRS has implemented capabilities to monitor and detect exfiltration as described below, with the exception of capabilities for digital rights management. Following the Get Transcript application incident in Fiscal Year 2015, the IRS has also taken steps to strengthen its network monitoring abilities. Recent TIGTA audit work[5] identified that following the online deployment of the Get Transcript application, automated attacks in Fiscal Years 2015 and 2016 were successful in gaining access to sensitive taxpayer information and had persisted for a period of months undetected because of the lack of sufficient network monitoring and coordinated audit log analysis. Automated attacks had also been successful in obtaining Social Security Numbers and Identity Protection Personal Identification Numbers through two additional online applications on IRS.gov (the IRS's public Internet site). The IRS has since initiated several actions to implement tools and harden its network operations against automated attacks. The IRS is also in the process of developing the infrastructure needed to analyze large volumes of data across the IRS and track end-to-end access and usage of online applications for quicker detection of malicious activity and fraudulent transactions occurring over the network. TIGTA is planning a follow-up audit in Fiscal Year 2017 to determine whether the IRS's efforts to strengthen its network monitoring controls were effective.

[4] TIGTA, Ref. No. 2013-20-025, *Desktop and Laptop Software License Management Is Not Being Adequately Performed* (June 2013); TIGTA, Ref. No. 2014-20-002, *The Internal Revenue Service Should Improve Mainframe Software Asset Management and Reduce Costs* (Feb. 2014); and TIGTA, Ref. No. 2014-20-042, *The Internal Revenue Service Should Improve Server Software Asset Management and Reduce Costs* (Sept. 2014).
[5] TIGTA, Audit No. 201520006, *Improvements Are Needed to Strengthen Electronic Authentication Process Controls.*

Capabilities for data loss prevention

The IRS has implemented a data loss prevention solution to monitor outbound e-mail and web transmissions. The solution blocks outbound unencrypted e-mail containing Social Security Numbers, system credentials, and passwords. It also blocks web transmissions of unencrypted Social Security Numbers.

In September 2014, TIGTA reported[6] on the development of the IRS's data loss prevention solution and found that it was identifying possible data loss incidents and the operational assessment team was correctly classifying 94 percent of our sampled events. TIGTA is planning a follow-up audit in Fiscal Year 2017 to determine the effectiveness of controls to prevent data loss, including any large-scale data exfiltration, of sensitive information.

Capabilities for forensics and visibility

The IRS Computer Security Incident Response Center (CSIRC) provided the following list of forensics and visibility capabilities. However, a recent CSIRC Quarterly Operational Review identified that CSIRC Operations has lost 30 percent of its staff since March 2015, resulting in reduced cyber incident monitoring, response capabilities, and customer support.

- **24 x 7 x 365 Operations Floor.** The CSIRC maintains continuous, proactive, near-real-time monitoring to prevent, detect, and respond to computer security incidents targeting the IRS enterprise information technology assets.
- **Firewall Rule Oversight/Approval Process.** The CSIRC reviews all requests for changes to IRS firewall rules and policies. After evaluating the security risks associated with the requests, the CSIRC then approves or denies the request. This provides the CSIRC with visibility into the expected, approved traffic traversing within/into/from the IRS network. This capability also provides the CSIRC with the opportunity to deny requests that may lower the IRS's security posture and often times with the opportunity to provide customers with a better, more secure solution to meet their needs.

  During Fiscal Year 2016, TIGTA audit work[7] determined that the IRS needs to improve firewall settings by removing unnecessary legacy firewall rules that are no longer needed and ensuring that only transmissions approved in a current Interconnection Security Agreement are allowed through the firewalls.
- **Web Proxy, Content Filtering and Blocking, and Approval Process.** The CSIRC uses web proxy servers to have full visibility into the web traffic leaving and entering the IRS network. The content filtering capabilities of the web proxy servers enable the CSIRC to

[6] TIGTA, Ref. No. 2014-20-087, *While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget* (Sept. 2014).
[7] TIGTA, Audit No. 201620006, *Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners.*

prevent user access to malicious websites and content. In addition, antivirus detection enables proactive blocking of malware based on custom rules. The CSIRC also has a process for allowing users to request access to restricted websites. This approval process provides the CSIRC with the opportunity to evaluate any potential security risks or violations of IRS policies before granting access to the sites.

- **E-Mail Gateway With Security Monitoring and Blocking.** The CSIRC uses e-mail gateways to have visibility into inbound and outbound traffic, including e-mail traffic between other Department of the Treasury bureaus. This capability allows the CSIRC to maintain policies that dictate the types of files allowed to traverse the gateways within e-mails, monitor for and prevent malicious e-mail–based activity, detect various types of e-mail abuse, and ensure that all IRS e-mail is acceptable.
- **Network Intrusion Detection.** The CSIRC uses network-based intrusion detection to monitor IRS network traffic, with the goal of identifying malicious traffic, policy violations, and other anomalous network behavior. This provides more in-depth visibility into the current state of the IRS network traffic flow and provides the opportunity to proactively monitor specific traffic that may be of interest based on current security trends and postures.
- **Host-Based Intrusion Detection.** The CSIRC uses host-based intrusion detection to have more insight into the security posture of hosts on the network. This capability provides an added layer of protection (in addition to the network-based intrusion detection), as more host-specific information is available for analysis. The CSIRC gains visibility into local changes made to a system and traffic to and from systems and has the ability to monitor role-specific activity, such as the activity of critical systems.
- **Packet Capture.** The CSIRC uses packet capture to maintain packet-level visibility of IRS network traffic. This capability provides security analysts with the ability to analyze network activity after sessions have occurred. This replay ability proves valuable when analyzing malicious activity for the purpose of gaining an understanding of exactly what occurred and also provides the ability to preserve data for auditing purposes and requirements.
- **Threat Intelligence Team.** The CSIRC's Threat Intelligence Team uses a threat intelligence capability to stay connected to the intelligence community for information sharing. This capability works on identifying advanced persistent threat actors targeting IRS assets and people. The CSIRC uses this intelligence to write custom rules and blocks throughout its security tool suites to better protect and safeguard IRS employees and taxpayers and their data.

During Fiscal Year 2016, TIGTA started an audit of the IRS's CSIRC Operations and plans to issue a report by February 2017.

Capabilities for digital rights management

The IRS has not implemented digital rights management capabilities. The IRS has discussed digital rights management with the Department of the Treasury and internally, but a schedule for implementation has not been developed.

Policies and Procedures With Respect to Ensuring That Entities, Including Contractors, That Provide Services to the IRS Are Implementing the Above-Mentioned Information Security Management Practices

The IRS requires contractors that provide services to the IRS using IRS-owned equipment to adhere to Internal Revenue Manual Section 10.8.1, *Information Technology Security Policy and Guidance*, which has been restructured and aligned to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.[8] Under Internal Revenue Manual Section 10.8.1, contractors are required to implement the above-mentioned information security management practices related to access controls (including multifactor authentication using PIV cards that comply with HSPD-12), software and licensing inventories, and network monitoring.

The IRS issued Publication 4812, *Contractor Security Controls*, for contractors that provide services to the IRS using their own systems (external contractors). The security controls contained in Publication 4812 are a subset of the NIST SP 800-53, Revision 4, and Internal Revenue Manual Section 10.8.1 control requirements for a moderate-impact system. This subset includes comparable, but not always identical, controls for access, software and licensing inventories, and network monitoring. The IRS did not intend Publication 4812 to require external contractors to implement controls identically to the IRS environment. The IRS indicated that, while Internal Revenue Manual Section 10.8.1 and Publication 4812 are both based on NIST SP 800-53, Revision 4, they apply to different operating environments, which are internal and external to the organization, respectively; and, as would be expected, vary greatly in the level of direct control the agency has over the service providers' normal business operations.[9]

The IRS indicated that contractor sites and work environments that use information technology assets to access, process, manage, or store sensitive information under contracts to the IRS will likely vary in size, number of users, and complexity. For this reason, the IRS established minimum and advanced sets of security controls that are selected depending upon the complexity of the contract, cost, and other factors. Federal guidance provides for agencies to consider such

[8] NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013) (includes updates as of 01-15-2014).

[9] NIST SP 800-53, Rev. 4 provides that small (business) contractors may not be large enough or sufficiently resourced to have elements dedicated to providing the range of security capabilities that are assumed by the baseline sets of security controls. Organizations consider such factors in their risk-based decisions.

risk factors when determining baseline security controls for the external entities that handle Federal agency data.

**********[10]**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********. During Fiscal Year 2016, TIGTA started a follow-up audit of patching and vulnerability management for public portal servers and should be issuing a report by February 2017.

[10] **********2**********
**********2**********
**********2**********
**********2**********.

Appendix I

Detailed Objective, Scope, and Methodology

Title IV of the Cybersecurity Act of 2015,[1] Section 406, *Federal Computer Security*, mandated Inspectors General to submit a report to the committees of jurisdiction in the Senate and the House of Representatives on specific information security management practices. The overall objective of this review was to provide the information requested by the Cybersecurity Act of 2015. To accomplish our objective, we:

I. Identified the policies and practices on system logical access,[2] including two-factor authentication to IRS systems for general and privileged users, and determined whether the policies are implemented.

   A. Described the logical access policies and practices used by the IRS to access a covered system.

   B. Described and listed the logical access controls and multifactor authentication used by the IRS to control access to covered systems by privileged users.

   C. Determined how the IRS ensures that these policies and procedures are being followed by employees.

   D. If the above policies and procedures were not implemented, we determined why.

II. Identified policies and procedures for maintaining an inventory of software and their licenses. If no inventory existed or it was not complete, we determined why.

III. Identified the methods used to monitor and detect exfiltration of sensitive data.

   A. Determined how the IRS uses the following technologies.

      1. Data loss prevention.

      2. Forensics and visibility.

      3. Digital rights management.

   B. If these technologies were not used, we determined why.

   C. Described the policies and procedures to ensure that entities, including contractors, that provide Cybersecurity services to the IRS are implementing information security management practices.

[1] Pub. L. No. 114-113, Division N § 406 (2015).
[2] See Appendix IV for a glossary of terms.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the Internal Revenue Manual sections relevant to IRS cybersecurity policies and procedures for access controls, software and software license management, network monitoring, and contractor security controls. We evaluated these controls by interviewing IRS Cybersecurity function personnel and reviewing relevant IRS documents.

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Bret Hunter, Senior Auditor
Midori Ohno, Senior Auditor
Esther Wilson, Senior Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Associate Chief Information Officer, Cybersecurity
Director, Office of Audit Coordination

Appendix IV

Glossary of Terms

Term	Definition
Active Directory	A directory service from Microsoft that is a part of Windows Server. It is an implementation of Internet standard directory and naming protocols that uses a database engine for transactional support and also supports a variety of application programming interface standards.
Advanced Persistent Threat Actors	An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objective by using multiple attack vectors (*e.g.*, cyber, physical, and deception).
altSecurityID Attribute	This attribute specifies a given user mapping for [X509] certificates or external Kerberos user accounts for the purpose of authentication.
Antivirus	Detects, prevents, and removes viruses, worms, and other malware from a computer. Antivirus programs include an auto-update feature that permits the program to download profiled or new viruses, enabling the system to check for new threats.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Authentication	The process of verifying that a claimed identity is genuine and based on valid credentials.
Certificate Mapping	Allows mapping between user accounts and digital certificates. This is useful when an organization issues client certificates to users. Client certificates are digital certificates that verify the identity of client software (web browsers) belonging to users.
Computer Security Incident Response Center	Part of the IRS Information Technology organization's Cybersecurity function. The CSIRC's mission is to ensure that the IRS has a team of capable "first responders" who are organized, trained, and equipped to identify and eradicate cyber threats or cyber-attacks. One of the primary duties of the CSIRC is to perform 24-hour monitoring and support to IRS operations seven days a week, 365 days a year. In addition, the CSIRC coordinates potential cybercrimes with TIGTA's Office of Investigations, Electronic Crimes and Intelligence Division, for further investigation and legal proceedings.

Term	Definition
Content Filtering and Blocking	The process of monitoring communications such as e-mail and webpages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users.
Covered System	A national security system as defined in § 11103 of title 40, U.S.C., or a Federal computer system that provides access to Personally Identifiable Information.
Credentials	See Identity Credential.
Cross-Agency Priority Goals	High-priority metrics set by the Administration to measure Federal agencies' success in improving the security of their information operations. These goals include metrics for implementing PIV cards. Also called cybersecurity cross-agency priority goals.
Digital Certificate	A digital representation of information used in conjunction with a public key encryption system, which at a minimum: 1. Identifies the certification authority issuing it. 2. Names or identifies its subscriber. 3. Contains the subscriber's public key. 4. Identifies its operational period. 5. Is digitally signed by the certification authority issuing it.
Digital Rights Management	A digital rights management shared service capability could enable a systematic approach to data-level protection across the Federal Government and help prevent unauthorized review, redistribution, and modification of sensitive Government information. While protections at the network level remain essential, adding protection at the data level is critical to achieving defense in depth.
E-Mail Gateway	An appliance-based security solution placed between the IRS network and the outside network, such as the Internet, that serves as a spam blocker and scans for viruses.
Encrypted	The process of converting plain text to cipher text by means of a cryptographic system.
End-to-End Security	Safeguarding information in an information system from point of origin to point of destination.
Exfiltration	The unauthorized transfer of information from an information system.

Term	Definition
Firewall	Software used to maintain the security of the IRS's network by blocking unauthorized network traffic to or from IRS systems. It is employed to prevent unauthorized web users or illicit software from gaining access to the IRS network that is connected to the Internet. It is the first line of defense in securing sensitive information. The IRS has installed firewalls at its connections with the Internet, its business partners, and its internal network.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Forensics	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Grid Card (also called Grid Authorization)	A method of securing user logons by requiring the user to enter values from specific cells in a grid whose content should only be accessible to the user and the service provider. Because the grid consists of letters and numbers in rows and columns, the method is sometimes referred to as bingo card authentication.
Host	Workstation or server.
Host-Based Intrusion Detection	Monitors a computer system to detect an intrusion or violation of the system's security policies and responds by logging the activity and notifying the designated authority. This tool has the ability to monitor key system files and any attempts to overwrite these files.
Hostname	The unique name by which a computer is known on a network.
Identity Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by an entity.

Term	Definition
Identity Protection Personal Identification Number (IP PIN)	To provide relief to tax-related identity theft victims, the IRS issues an IP PIN to taxpayers who are confirmed by the IRS as victims of identity theft and taxpayers who are at a high risk of becoming a victim, such as taxpayers who call reporting a lost or stolen wallet or purse as well as taxpayers who live in three locations that the IRS has identified as having a high rate of identity theft (Florida, Georgia, and the District of Columbia). Taxpayers who receive the six-digit IP PIN must use it on electronic and paper returns in order for the returns to be accepted for processing.
Internet Protocol Address	An Internet Protocol address is an identifier for a computer or device on a suite of communication protocols used to connect hosts on the Internet. The format of an Internet Protocol address is a 32-bit numeric address written as four numbers separate by periods. Each number can be zero to 255.
Logical Access	Interactions with hardware through remote access. This type of access generally features identification, authentication, and authorization protocols. It is contrasted with the term "physical access," which refers to interactions with hardware in the physical environment where equipment is stored and used.
Multifactor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (1) something you know (*e.g.*, password); (2) something you have (*e.g.*, cryptographic identification device, token); or (3) something you are (*e.g.*, physical characteristic).
Packet, Packet Capture	Intercepts and analyzes a data packet crossing or moving over the IRS's network. The packet is inspected to help diagnose and solve network problems and determine whether security policies are being followed. Packet capture can be used to identify security flaws and breaches by determining the point of intrusion, identifying data leakage by analyzing and monitoring content to determine leakage points and sources, and forensic investigations.
Patch, Patching	An update to an operating system, application, or other software issued specifically to correct particular problems with the software.
Personal Identity Verification Card	A U.S. Federal smart identification card that contains the necessary data for the cardholder to be granted access to Federal facilities and information systems and assure appropriate levels of security for all applicable Federal applications.

Term	Definition
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity (name, Social Security Number, biometric records, *etc.*), alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (date and place of birth, mother's maiden name, *etc.*).
Privileged Accounts/Users	Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts.
Public Portal Servers	A network server that deploys portal services to a public website or internal intranet. A portal is a website that aims to be an entry point to the World Wide Web.
Remote Access	Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (*e.g.*, the Internet).
Sensitive But Unclassified	Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction.
Threat Intelligence	Also known as cyber threat intelligence is organized, analyzed, and refined information about potential or current attacks that threaten an organization.
Token	Something that the claimant possesses and controls (typically a key or password) that is used to authenticate the claimant's identity.
Visibility Capabilities	Network visibility tools that help security professionals discover things about the network and user behavior that can help bolster security policies.
Web Proxy	A server that filters and evaluates each Internet address and request when a user accesses a file or opens a web page.