TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Security Over High Value Assets Should Be Strengthened

May 18, 2018

Reference Number: 2018-20-029

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.

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.

SECURITY OVER HIGH VALUE ASSETS SHOULD BE STRENGTHENED

Highlights

Final Report issued on May 18, 2018

Highlights of Reference Number: 2018-20-029 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

Across the Federal Government, agencies operate High Value Assets (HVA) that contain sensitive information or support critical services. HVAs enable the Government to conduct essential functions and operations, provide services to citizens, generate and disseminate information, and facilitate greater productivity.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the IRS's efforts in implementing controls to protect its HVAs.

WHAT TIGTA FOUND

On January 13, 2017, the Department of the Treasury notified the IRS that two of its 47 systems identified as HVAs were included in a list of Treasury Department HVAs being reported to the Department of Homeland Security. Currently, the focus of the HVA effort is at the department level, and the Treasury Department has yet to issue formal guidance to its bureaus.

In the interim, the IRS stated that it is meeting the Office of Management and Budget Cybersecurity Strategy and Implementation Plan recommendations and requirements related to HVAs with its Federal Information Security Modernization Act program and has risk management processes and initiatives in place to enhance the security of its HVAs. However, due to the mission-critical nature of the IRS's HVAs to tax administration, additional steps are needed to ensure that defined processes and security controls are strengthened.

Specifically, the IRS has not taken actions related to the Cybersecurity Strategy and Implementation Plan to identify and document all of its current system hardware components and further protect its HVAs. Although the IRS stated that it has initiatives in place that will help identify its hardware components, not all system boundary components were accurately identified.

The IRS has not conducted HVA efforts to implement the Cybersecurity Strategy and Implementation Plan requirements to inventory and validate the system access capabilities and the number of privileged accounts as well as minimize the number of privileged users to specific HVAs. However, the IRS stated it has established repeatable processes for monitoring, tracking, reviewing, approving, and reducing elevated access. Nonetheless, when requested, the IRS could not readily identify all individuals who have privileged access to its HVA components.

Further, the IRS did not effectively and timely mitigate critical and high-risk vulnerabilities in one of its HVAs. The IRS also did not capture, verify, or maintain historical data on patch implementation dates for any active or retired servers or identify trends in its patch management program until December 2017.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer implement actions to identify and document current system hardware components for all IRS HVAs, automate the process that identifies privileged users and their approved privileged access authorizations to enhance the IRS's ability to validate system access to HVAs and minimize access inventory, and ensure that patching of security vulnerabilities is completed within the required 30-calendar-day time frame.

The IRS agreed with all recommendations. The IRS plans to continue its efforts to identify and document current system hardware for IRS information systems; develop a strategy and implement a process to more effectively manage and monitor privileged access; and complete the approved patch management process to ensure that patching of security vulnerabilities is completed within the required time frame.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

May 18, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Security Over High Value Assets Should Be Strengthened (Audit # 201720016)

This report presents the results of our review to evaluate the Internal Revenue Service's efforts in implementing controls to protect its high value assets. This audit is included in our Fiscal Year 2018 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of Internal Revenue Service Resources.

Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Abbreviations

CSIP	Cybersecurity Strategy and Implementation Plan
FISMA	Federal Information Security Modernization Act of 2014
HVA	High Value Asset
IDRS	Integrated Data Retrieval System
IMF	Individual Master File
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
OMB	Office of Management and Budget

Background

In June 2015, the U.S. Office of Personnel Management announced that it had been the target of a data breach[1] involving the records of as many as 21.5 million people. It discovered that the background investigation records of current, former, and prospective Federal employees and contractors (and nonapplicants, *e.g.*, primarily spouses or cohabitants of applicants) had been stolen. The data breach appeared to have started in May 2014 but was not noticed by the Office of Personnel Management until April 2015. Information targeted in the breach included Personally Identifiable Information, such as Social Security Numbers, names, addresses, and dates and places of birth. It is estimated that this data breach could cost the Government more than $1 billion in identity monitoring services, *e.g.*, credit monitoring services, over the next decade.

Consequently, on June 12, 2015, the Federal Chief Information Officer initiated a Cybersecurity Sprint that required agencies to take immediate steps to further protect Federal information and assets as well as improve the resilience of Federal networks. In addition to providing direction to agencies, the Federal Chief Information Officer established a Cybersecurity Sprint team to lead a 30–calendar-day review of the Federal Government's cybersecurity policies, procedures, and practices. The team was also tasked with creating and implementing a set of action plans and strategies to further address critical cybersecurity priorities and recommend a Federal civilian cybersecurity strategy.

The Cybersecurity Sprint team's recommendations resulted in the Office of Management and Budget (OMB) issuing Memorandum 16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, on October 30, 2015. The OMB Cybersecurity Strategy and Implementation Plan (CSIP) provides guidance that included recommendations and requirements on strengthening Government processes for developing, implementing, and institutionalizing best practices; developing and retaining the cybersecurity workforce; working with public and private sector research and development communities to leverage the best of existing, new, and emerging technology; and identifying and protecting High Value Assets (HVA).

Across the Federal Government, agencies operate HVAs that contain sensitive information or support critical services. HVAs enable the Government to conduct essential functions and operations, provide services to citizens, generate and disseminate information, and facilitate greater productivity. Federal agencies have taken steps to identify, categorize, and secure their information technology assets whose confidentiality, integrity, and availability are essential to their ability to operate and execute their missions. In recent years, continued increases in

[1] See Appendix IV for a glossary of terms.

computing power combined with declining computing and storage costs and increased network connectivity have expanded the Government's capacity to store and process data in order to improve service delivery to the public. This increased reliance on technology and interconnectivity also means that the Government's critical networks, systems, and data are more exposed to cyber risks. Therefore, the Government must continue to evolve its approach to managing the risks to these HVAs and document a continuous review of all critical networks, systems, and data.

The Department of the Treasury identified the Internal Revenue Service's Integrated Data Retrieval System and the Individual Master File as part of its Top 10 list of High Value Assets.

Accordingly, the Department of the Treasury began efforts to identify all of its HVAs in July 2015. The Treasury Department's Cybersecurity organization issued information requests to each Treasury Department bureau, including the Internal Revenue Service (IRS). The Treasury Department performed an analysis to identify its HVAs in conjunction with ongoing Cybersecurity Sprint activities and the information provided by its bureaus. On January 13, 2017, the Treasury Department notified the IRS that two of its systems, the Integrated Data Retrieval System (IDRS) and the Individual Master File (IMF), were identified for inclusion in a Top 10 list of Treasury Department HVAs being reported to the Department of Homeland Security as required by OMB Memorandum 17-09, *Management of Federal High Value Assets*, dated December 9, 2016. The Department of Homeland Security and the OMB used this information to review and prioritize all of the Federal Government's civilian HVAs. Based upon these reviews, four high-priority Treasury Department HVAs, including the IDRS and the IMF,[2] were subjected to risk vulnerability assessments.

This review was performed in the IRS Information Technology organization's Applications Development, Cybersecurity, and Enterprise Operations organizations at the New Carrollton Federal Building in Lanham, Maryland, during the period February 2017 through January 2018. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective. However, we were limited in our testing to determine whether the IRS timely applied critical and high-risk security patches to its servers in the Tier II environment because the IRS did not begin capturing the patch implementation dates until July 2017. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[2] The remaining two high-priority HVAs are non-IRS systems.

Results of Review

The Treasury Department coordinated with the IRS on the identification of its HVAs and continues to work with the IRS on criteria for refining and designating new potential HVAs. IRS Cybersecurity personnel responded to two information requests from the Treasury Department's Cybersecurity organization and continue to attend regularly scheduled HVA meetings with the Treasury Department. The information requests and meetings provide the Treasury Department an opportunity to share information on its HVA efforts with its bureaus and, in return, receive information from its bureaus on their systems for analysis in identifying their HVAs.

Using information obtained from the Treasury FISMA [Federal Information Security Modernization Act of 2014][3] Inventory Management System, the Treasury Department initially identified 142 IRS systems that potentially store and process Personally Identifiable Information. The first information request asked the IRS to validate that the system list was accurate and complete as well as to provide the number of records containing Personally Identifiable Information for each system. Based on this information and additional analysis, the Treasury Department narrowed the list to 124 IRS systems. For its second information request, the Treasury Department asked for information on the security controls assessments for each of the 124 IRS systems. Requested information included the date of the last security controls assessment, summary results of the assessment, and plan of action and milestones information to correct open weaknesses concerning nine specific security controls.[4] Based on this information, the Treasury Department ultimately identified 47 HVAs at the IRS.

In addition, the IRS collaborated with the Department of Homeland Security during risk vulnerability assessments of the IDRS and the IMF. The Department of Homeland Security identified two medium-severity rated findings, one related to an exposed administrative interface and the other related to the susceptibility of IRS employees to spear phishing. Once notified of the risk vulnerability assessment results, the IRS stated that it immediately corrected the exposed administrative interface and is relying on the Treasury Department's ongoing campaign to test its employees to address the spear phishing finding.

Currently, the focus of the HVA effort is at the department level, and the Treasury Department has yet to issue formal guidance to its bureaus. In the interim, the IRS stated that it is meeting CSIP recommendations and requirements related to HVAs with its FISMA program and has risk management processes and initiatives, *e.g.*, vulnerability scanning and penetration testing, in

[3] Pub. L. No. 113-283. This bill amends Chapter 35 of Title 44 of the United States Code to provide for reform to Federal information security.

[4] The nine security controls are: 1) risk assessment, 2) emergency power, 3) account management, 4) boundary protection, 5) malicious code protection, 6) system interconnections, 7) incident response plan, 8) alternate processing site, and 9) information system recovery and reconstitution.

place to enhance the security with not only HVAs but all of its FISMA systems. However, due to the mission-critical nature of the IRS's HVAs to tax administration, additional steps are needed to ensure that defined processes and security controls are strengthened.

Defined Processes and Security Controls Need to Be Strengthened

Strengthening the cybersecurity of networks, systems, and data is of the utmost importance. As a result, the Cybersecurity Sprint, led by the OMB, required agencies to take immediate steps to further protect Federal information and assets and improve the resilience of Federal networks. These actions included identifying high-value information and mission-essential assets, inventorying and validating the system access capabilities and the numbers of privileged accounts, reviewing and reducing the number of privileged users, and patching critical vulnerabilities.

The inventory of IRS HVA components is not accurate

The first of five OMB CSIP objectives intended to strengthen Federal civilian cybersecurity, *i.e.*, ***prioritized identification and protection of high-value information and assets***,[5] requires agencies to identify the value and impact of the information on their systems and networks. Agencies must then identify the information technology assets used to store, process, and transmit that information. Agencies must also identify those assets and capabilities that enable mission-essential functions and ensure delivery of critical services to the public. Once an agency has identified and inventoried its HVAs, it must protect them with a variety of policies, processes, and tools as well as maintain a current inventory of hardware components. Furthermore, agencies will continue to identify their HVAs and critical system architectures in order to understand the potential impact to those assets from cyber incidents and ensure that robust physical and cybersecurity protections are in place.

In addition, the Internal Revenue Manual (IRM)[6] provides that system security plans are to be reviewed annually (at a minimum) or as a result of any significant change. System security plans will be updated to address changes to the information system or environment of operation or problems identified during plan implementation or security controls assessments. Examples of significant changes to an IRS information system include, but are not limited to: 1) installation of a new or upgraded operating system, middleware component, or application or 2) installation of a new or upgraded hardware platform or firmware component.

[5] The remaining four objectives are: 1) *timely detection of and rapid response to cyber incidents*, 2) *rapid recovery from incidents when they occur and accelerated adoption of lessons learned from the Sprint assessment*, 3) *recruitment and retention of the most highly qualified cybersecurity workforce talent the Federal Government can bring to bear*, and 4) *efficient and effective acquisition and deployment of existing and emerging technology*.

[6] IRM 10.8.1, *Information Technology Security, Policy and Guidance* (July 8, 2015).

The IRS has not taken actions related to the OMB CSIP to identify and document all of its current system hardware components and further protect its HVAs. Instead, the IRS stated that it has risk management initiatives in place that will help identify its hardware components. These include:

- Continuous Diagnostics and Mitigation, the foundation of which is hardware and software asset management, is scheduled for implementation in Fiscal Year 2018.
- Contingency Planning, which collects Internet Protocol addresses that identify hardware components through its system contingency planning testing exercises.
- The System Interconnection process, which enhances the coordination between employees involved with documenting system interconnections and employees involved with establishing these interconnections.

In addition, the IRS stated that it has a comprehensive FISMA program which meets the requirements of the CSIP and includes an inventory of systems that has been designated as HVAs. The IRS referred us to its system security plans that document related system boundary components in the system environment and system interconnections.

We reviewed the IDRS and the IMF system security plans dated November 9, 2016, and October 17, 2016, respectively, and found that not all system boundary components were accurately identified, nor was the IDRS system security plan updated when a significant change was made to the inventory of components within the system environment. Specifically, an IDRS primary mainframe was replaced in December 2016, and the IDRS system security plan was not updated as required. Similarly, four servers were retired (two in December 2011, one in May 2012, and one in August 2013) but remain listed in the most current IDRS system security plan.

Moreover, the Customer Account Data Engine 2 database is not identified either as within or as an interconnecting system outside the system environment in both the IDRS and the IMF system security plans. The Customer Account Data Engine 2 is the ongoing modernization effort for the IMF and currently serves as the point of access to the IDRS for the IMF data; as such, it should have been identified as an interconnecting system in both system security plans. In November 2017, the IRS updated both system security plans to reflect the changes in the inventory of components we identified.

Additionally, the accuracy of the IRS's system components was questioned in TIGTA's last two annual audits of the IRS's FISMA program.[7] In Fiscal Year 2016, we reported that while the IRS had implemented an asset management solution as its official inventory solution, the

[7] TIGTA, Ref. No. 2016-20-092, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2016* (Sept. 2016), and TIGTA, Ref. No. 2017-20-087, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Sept. 2017).

inventory was not accurate or incomplete. A review of the system security plans determined that the security control over the system boundary components was not fully in place for three of the 10 systems selected for review. In addition, in Fiscal Year 2017, we reported that the IRS did not maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.

IRS Cybersecurity personnel stated that, as the owner of the FISMA program, the Cybersecurity organization is responsible for ensuring that the system security plans accurately reflect the system. IRS Cybersecurity personnel also stated that the system security plans are static, reviewed annually (at a minimum), and updated as needed. System security plans can also be updated during ad-hoc security controls assessments when a change occurs requiring an assessment. In addition, the system owner is responsible for updating the system security plan when changes occur outside of the security control assessment cycle. Currently, this is a paper-driven process, which may allow for gaps in updates. However, both Cybersecurity personnel and the system owners of the IDRS and IMF failed to update the system security plans as required. The IRS cannot begin efforts to fully protect its mission-critical HVAs, *e.g.*, the IDRS and the IMF, if the IRS's system hardware components are not accurately identified and inventoried.

Recommendations

The Chief Information Officer should:

Recommendation 1***:*** Implement the OMB CSIP actions to identify and document current system hardware components for all IRS HVAs.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS Information Technology organization will continue efforts already underway to identify and document current system hardware for IRS information systems, including HVAs.

Recommendation 2: Develop an effective process to update the IDRS and the IMF system security plans, including any system changes outside of the security control assessment cycle.

> ***Management's Response:*** The IRS agreed with this recommendation. The Information Technology Cybersecurity organization will improve upon its process to update the IDRS and IMF system security plans. These updates will be required to occur following scheduled assessments and system changes outside of the security controls assessment cycle. This change will take effect starting with the FISMA 2019 review cycle.[8]

[8] The FISMA 2019 review cycle is July 1, 2018, through June 30, 2019.

Users with privileged access to IRS HVA components cannot be readily identified

The OMB CSIP initiated protection activities to improve Federal cybersecurity included strengthening controls over privileged access in the areas of policies, practices, and procedures. Accordingly, the OMB CSIP required agencies to immediately review policies and practices for privileged users and for agencies to continue:

- Inventorying and validating the system access capabilities and the number of privileged accounts.
- Minimizing the number of privileged users.
- Limiting functions that can be performed when using privileged accounts.

In addition, IRM 10.8.1 provides that the IRS shall identify information system account types to support organizational missions and business functions and review privileged accounts semiannually (at a minimum) for compliance with account management requirements. Employees who perform multiple roles and tasks shall have separate user accounts for each. Additionally, accounts with privileged access shall be prohibited from web browsing and other Internet connections. The Service-Wide Online 5081 system shall be used to register all users for access to any IRS information technology asset for which they require access, and each information technology asset for which a user has been granted access shall be identified, documented, and authorized by the user's manager.

The IRS cannot readily identify all individuals who have privileged access to its HVA components because it does not maintain a complete inventory listing of privileged users and accounts specific to an HVA. Enterprise Operations personnel were not able to provide a complete inventory listing of users and accounts with privileged access to the IDRS and the IMF as of March 1, 2017. The IDRS and the IMF system security plans identified 13 hardware components composing of 37 servers (including virtual, partitioned, systems development, testing, and disaster recovery servers). It took the IRS over three months to provide a partial listing of privileged users and accounts for only 10 (30 percent) of the 33 servers.[9] Given that the IRS has not been able to provide this basic but critical information, we question whether the IRS has sufficiently inventoried, validated, and minimized the number of privileged users and accounts as required by the OMB CSIP or complied with its own requirements to review privileged accounts semiannually. Figure 1 presents the results of our request for privileged users and accounts by HVA.

[9] Four IDRS servers were retired: two virtual servers on December 13, 2011; one virtual server on May 16, 2012; and one production server on August 13, 2013.

Figure 1: Results of the Request for a Listing of HVA Privileged Users and Accounts

HVA	Hardware Components	Servers	Servers With Privileged Users and Accounts Data Provided	Servers With Privileged Users and Accounts Data Not Provided
IDRS	12	22	6 (27%) (all production)	16 (73%) (2 production and 14 nonproduction)[10]
IMF	1	11	4 (36%) (all production)	7 (64%) (all nonproduction)
TOTAL	**13**	**33**	**10 (30%)**	**23 (70%)**

Source: Treasury Inspector General for Tax Administration analysis of IRS documentation on the IDRS and the IMF privileged users and accounts.

The IRS has a supplemental process to document users' privileged access rights and roles to information technology assets, *e.g.*, servers and applications. Users requesting privileged access must first complete a privileged role request form that is used in documenting the approved privileged user's role and for managing and controlling the elevated access requests. This form lists the specific information technology asset(s) to which the user is requesting authorization for privileged access. After completion and approval of the form, the Online 5081 system is used to authorize and control the access to the privileged user role, but it does not specify the information technology asset. As of September 14, 2017, there were 366 approved privileged role request forms for all IRS information technology assets.

In order for us to verify whether the users are authorized and approved to have privileged access to a specific asset related to an HVA, each of the 366 approved privileged role request forms need to be manually reviewed. We would then need to capture the user role approved for privileged access by server name and reference the server name back to the list of servers supporting the HVA components and the approved privileged role back to the Online 5081 system. However, these forms are not maintained by user or server name but rather by division and group. A single form often contains multiple users requesting privileged access to multiple servers or applications.

To gauge the population scope and the time required to determine whether the privileged users are authorized, we conducted an initial assessment of the partial listing as of September 14, 2017, provided to us by the IRS. In our analysis of nine of the 10 IDRS and IMF servers for which data were provided,[11] we identified 1,053 users approved for privileged access. Due to the

[10] Nonproduction servers include development, testing, and disaster recovery servers.
[11] The IDRS and the IMF share four of the same servers.

volume and manual process necessary to verify whether a user is authorized and approved to have privileged access to a specific server, we conducted limited testing in this area by selecting a judgmental[12] sample of 10 privileged users for review. We found that the user role for all 10 privileged users were authorized and approved on a privileged role request form and on the Online 5081 system.

Additionally, to verify the IRS's compliance with IRM 10.8.1, we conducted limited testing to ensure that users with privileged access were restricted from web browsing or other Internet connections. We judgmentally selected a sample of eight users with privileged access and observed the user create a privileged session (*i.e.*, accessed the system via the privileged account) and attempt to access the Internet. We found that none of the users were able to browse the web or have other Internet connections from within their privileged session.

The Enterprise Operations organization stated that it has established repeatable processes for monitoring, tracking, reviewing, and approving elevated access. However, much of these processes are manual and vary based upon system type, *e.g.*, Unisys, Solaris, IBM. We previously discussed, in this report, the issues with the manual Online 5081 process for assigning privileged users in our attempt to validate user access to the IDRS and IMF HVAs. We also reported this issue in our Fiscal Year 2017 FISMA report stating that, for the IRS to meet an effective level for the identity and access management program area, the IRS needs to employ automated mechanisms to support the management of privileged accounts.

The IRS Enterprise Operations organization also stated that between Fiscal Years 2010 and 2017, the number of privileged users and accounts for its Tier II environment decreased from 4,638 to 726, a total reduction of 84 percent. The IRS's efforts of reducing privileged users and accounts is tracked in the Treasury Department's SharePoint Investment Knowledge Exchange system. We obtained the SharePoint Investment Knowledge Exchange system report as of January 2018 and confirmed the 726 total reported by the IRS.

In addition, the Enterprise Operations organization stated that it does not maintain historical information on nonproduction servers, only the current state of users having privileged access. This is concerning because live taxpayer data can be maintained on these servers. While historical information of privileged users and accounts on production servers is maintained, the IRS was not able to provide us privileged users and accounts information for two production servers. Further, we gave the IRS another opportunity to provide current privileged users and accounts information. The IRS still took approximately one month to provide this information. A different methodology was used to generate the data and complete source data were not provided to us. Because we were not provided complete source data, we could not determine their validity. As a result, we were unable to verify that the IRS has successfully taken steps to minimize the number of privileged users for its HVAs.

[12] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Privileged accounts are a known target for malicious actors. In the vast majority of security breaches, stolen credentials and privileged accounts continue to be the prime target for hackers because they unlock the access required to virtually exploit any part of an organization's network, including critical and sensitive data. Despite this, identifying and managing privileged users and accounts at the IRS still relies on manual, time-consuming tasks.

Recommendation

Recommendation 3*:* The Chief Information Officer should direct the Enterprise Operations organization to develop an approach and implementation timeline for how to automate the process that identifies privileged users and their approved privileged access authorizations to enhance the IRS's ability to validate system access to HVAs and minimize access inventory.

> ***Management's Response:*** The IRS agreed with this recommendation. The Enterprise Operations organization will develop a strategy and plan to implement a process to more effectively manage and monitor privileged access. The strategy and plan will include automating as much of the process as is achievable given technical, resource, and budget constraints.

The IRS did not effectively and timely mitigate critical and high-risk IDRS vulnerabilities

The IRM[13] provides that the IRS Computer Security Incident Response Center issues advisories to IRS organizations alerting them of significant threat or incident information. The advisories provide a vulnerability metric that measures the harm of the vulnerability if unpatched, the potential extent of the exposure, the criticality of the affected IRS system(s), and the assigned overall severity rating on the vulnerability as well as the established implementation schedule.[14] Any security patch designated as critical or high-risk needs to be implemented within 30 calendar days. The IRM also provides that the IRS's Patch and Vulnerabilities group or similar entity is responsible for identifying program metrics to help manage the strengths and weaknesses as well as trends in the IRS patch management program, the security posture of the enterprise, and the means of delivering these metrics. In addition, the IRM specifies that a tracking mechanism captures the IRS's compliance in meeting system security and the latest patching requirements.

Further, the IRM states that the Cybersecurity organization is responsible for collecting metric data on a monthly basis (at a minimum) for the following purposes: the annual FISMA reporting, the quarterly reports for senior leadership, the Treasury Department cyber analysis and

[13] IRM 10.8.50, *Information Technology Security, Servicewide Security Patch Management* (April 29, 2016).

[14] The IRM further provides that advisories published by the Computer Security Incident Response Center are not the all-inclusive authoritative source for vulnerabilities and patches. The advisories are to be used in collaboration with advisories from other relevant sources.

reporting dashboard, the IRS Information Technology organization's internal dashboard, and any ad-hoc reporting. The process and procedures for collecting patch and vulnerability metrics shall be defined in the standard operating procedures.

Tier I Environment

The IRS was updating and applying changes, *e.g.*, maintenance, fixes, modifications, and enhancements, to its mainframes in the Tier I environment that support the IDRS and the IMF.[15] According to the IRS, the process to update and apply system changes to its mainframes is more structured than its Tier II environment servers. Updates with the changes to the IBM and Unisys mainframes are typically scheduled every two years by the vendors. For the IBM mainframes, the updates are tested by the vendor and released in a bundled package that is automatically applied to the mainframe in coordination with the IRS. The updates are supported for the two releases from its current release version. For the Unisys mainframes, the updates are also tested by the vendor prior to release and are supported for two to two and a half years. The updates can be downloaded to an individual workstation computer and then electronically transferred to the mainframe where the software is maintained. From September 2015 to June 2017, there were four bundled updates consisting of 890 changes applied to the IBM mainframe and one operating system update and two bundled updates consisting of 60 changes applied to the Unisys mainframe.

Tier II Environment

The IRS cannot effectively manage its patch management program and identify trends if complete historical patch implementation data related to IDRS hardware components operating in the Tier II environment are not being captured.[16] For example, while the IRS stated that it had metrics tracking the implementation of patches since December 2016, the IRS does not capture, verify, or maintain historical data on patch implementation dates of any active or retired servers or identify trends in the patch management program. As a result, the IRS was not able to provide us with complete patch information for each of the hardware components identified in its IDRS system security plan. As of August 2, 2017, the IRS took over three months to provide patch information for 14 (78 percent) of the 18 identified hardware components related to the IDRS.

The Enterprise Operations organization's Infrastructure Risk Analysis Section is responsible for program oversight of all nonexecution functions of patch management, which includes generating patch schedules, notifications, coordination, and reporting. At the request of the Treasury Inspector General for Tax Administration audit team, the Infrastructure Risk Analysis Section provided a newly created and still-under-development *Patch Implementation Report* for

[15] The IRS does not use the term "patching" to describe its Tier I mainframes but rather uses the terms "updates" and "changes." In addition, the IRS does not differentiate these updates and changes to a specific system but to the mainframe that supports these individual systems and applications.

[16] The IMF system security plan provides that its infrastructure does not operate in the Tier II environment, only in the Tier I mainframe environment.

April 2017. No other metrics report regarding whether the IRS was complying with its 30–calendar-day requirement of patching critical and high-risk security patches existed prior to this *Patch Implementation Report*.

According to the IRS, to be compliant with the IRM, the report identified all patches released by vendors during the month of April 2017 as well as the number and percentage of outstanding and applied patches to the IRS's Tier II environment. The intended purpose of this report is to provide IRS management with a monthly status of the IRS's overall compliance with patch management. However, this report was not complete because it did not provide trends in patch compliance for patches released prior to June 2017 and it did not capture any patch implementation dates until July 2017. Based on the IRS not having an established process that measures patch management compliance and the fact that a report was newly created and still under development, our scope was limited to recent reports that contained the IRS patch implementation dates.

Based on our review of these reports, we found that the IRS was not always timely applying critical and high-risk security patches for its IDRS servers. In a *Patch Implementation Report* dated June 5, 2017, that included all outstanding patches,[17] the IRS reported that it had 77 outstanding IDRS security patches rated as critical and high-risk. Based upon our calculation between the patch release date and the date the report was created, our analysis determined that 37 (48 percent) of the patches were over-aged by an additional 25 calendar days.[18] These unpatched vulnerabilities related to servers running the Microsoft Windows 2003 operating system. This issue is consistent with findings reported in our last two FISMA reports that the IRS has not consistently implemented patches timely.

In a more recent report, dated July 24, 2017, the IRS stated that all critical and high-risk vulnerabilities related to the IDRS components were patched and that it was able to reduce the number of over-aged patches by applying the most recent patch first, when applicable, which encompasses all prior patch releases. The IRS also stated that it was able to retire or replace some older servers running Windows 2003. In addition, the IRS provided us a December 2017 report that presents trends in patch remediation along with the implementation date for each patch release.

According to the Infrastructure Risk Analysis Section manager, the IRS was addressing the patching constraints. Specifically, these constraints included a fragmented IRS patch management program with no executive or project accountability, incorrect server and software inventories, inconsistent and nonrepeatable patch reporting that also did not account for all systems and servers, and unknown patch success and failure rates, among other constraints.

[17] The *Patch Implementation Report* for April 2017 provided information on patches released by vendors only for the month of April 2017.

[18] The IRS considers any critical and high-risk security patches not applied within 30 calendar days to be over-aged.

However, the IRS stated that it does have tools and initiatives to help better manage its patch management program, including:

- Continuous Monitoring – Filing Season and Financial Systems Dashboards – provide an organizational view to help prioritize and direct remediation actions to fix vulnerabilities of critical applications and systems, including HVAs.
- Patch Management Dashboards – provide executive-level view of all patching statuses.
- Vulnerability Scanning – conducts network and operating system vulnerability checks against the complete enterprise twice per week.
- Ongoing Penetration Testing – tests, since October 2016, against its entire external perimeter to proactively identify vulnerabilities.

In addition, the IRS provided a *Patch Implementation Schedule* report, dated February 14, 2018, that will be used to track the implementation of patches against an approved schedule for the Linux, Solaris, and Windows systems. The report identifies the critical patch release date, the servers affected, and the status of the patch implementation and also captures the patch implementation date(s). The IRS stated that the new processes, *i.e.*, this report, should enable it to meet the 30–calendar-day compliance requirement.

Without effective patch management program metrics, the IRS cannot determine whether vulnerabilities are timely mitigated. Failure to timely remediate security vulnerabilities may allow known weaknesses to be exploited and could result in the loss or disruption of the IDRS or other systems that are critical to tax administration operations.

Recommendation

Recommendation 4***:*** The Chief Information Officer should direct the IRS Enterprise Operations organization to ensure that patching of security vulnerabilities is completed within the required 30–calendar-day time frame.

> ***Management's Response:*** The IRS agreed with this recommendation. The Enterprise Operations organization will complete the approved patch management process to ensure that patching of security vulnerabilities is completed within the required IRM time frame.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the IRS's efforts in implementing controls to protect its HVAs.[1] To accomplish our objective, we:

I. Assessed the status of efforts to identify the IRS's HVAs.

   A. Identified and reviewed OMB, Treasury Department, and IRS guidance, policies, and procedures on the HVA program as well as security controls over access management, security controls assessments, configuration management, and planning.

   B. Interviewed Treasury Department and IRS Cybersecurity organization officials as well as obtained and reviewed documentation to determine the:

      1. Status of the HVA program at the Treasury Department and the IRS.

      2. Treasury Department criteria used in identifying and selecting HVAs.

      3. Guidance provided to the IRS for the HVA program.

      4. Types of information requested from the IRS and information the IRS provided to the Treasury Department.

      5. IRS systems identified as HVAs and reported to the Department of Homeland Security.

II. Determined whether the IRS properly identified all components that compose the system boundary for the IDRS and the IMF.

   A. Reviewed the IRS documents used to support the identification of the system boundary for the IDRS and the IMF in response to OMB Memorandum 16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government* (October 2015).

   B. Validated the information obtained in Step II.A by reviewing additional documentation to ensure that all system components of the IDRS and the IMF were identified by the IRS.

   C. Interviewed IRS Cybersecurity personnel, IRS Enterprise Operations personnel, IDRS and IMF business stakeholders, and IDRS and IMF Applications Development

[1] See Appendix IV for a glossary of terms.

personnel to determine the IDRS and IMF missions as well as the IRS operating unit business requirements and processes to ensure that all system components used in meeting these commitments have been identified.

III. Determined whether the IRS has timely applied vendor security patches to secure all system components of the IDRS and the IMF.

A. Researched vendor websites for all system components identified from Step II to identify critical and high-risk security patches and version release schedules from October 2015 to May 2017.

B. Reviewed documentation obtained from Enterprise Operations personnel to determine when security patches were applied to system components selected for review. We were unable to validate the accuracy and completeness of the *Patch Implementation Reports* to prior patch information obtained from the IRS due to the timing of the reports.

C. Determined whether the IRS timely applied security patches by calculating the number of days between the vendor security patch release dates and the dates the IRS applied the security patches.

IV. Evaluated the IDRS and the IMF privileged account administration to determine whether privileged users and accounts were authorized and reviewed.

A. Determined whether IDRS and IMF privileged users and accounts were authorized.

1. Obtained a listing of all current privileged users and accounts on each system component identified in Step II.

2. Selected a judgmental sample[2] of 10 privileged users and accounts to determine whether they were authorized and approved on a privileged role request form and on the Online 5081 system.

B. Evaluated the management of IDRS and the IMF privileged users and accounts in response to the OMB CSIP required actions for agencies to immediately review policies and practices for privileged users. Specifically, we determined whether the IRS:

1. Inventoried and validated the system access capabilities and the number of privileged accounts by requesting an inventory of privileged users with access to the servers identified in the IDRS and the IMF system security plans as of March 31, 2017.

2. Minimized the number of privileged users.

[2] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

3. Limited functions that can be performed when using privileged accounts. We assessed this by observing a judgmental sample of eight privileged users logging into privileged sessions and trying to browse the web or access other Internet connections.

V. Determined whether the IRS addressed and corrected the vulnerabilities identified in the Department of Homeland Security risk vulnerability assessments of the IDRS and the IMF.

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: OMB Memorandum 16-04; OMB Memorandum 17-09, *Management of Federal High Value Assets* (December 2016); and the IRM. We evaluated these controls by interviewing Treasury Department personnel and IRS Cybersecurity, Applications Development, and Enterprise Operations office personnel and by reviewing system security plans, patch reports, and privileged role requests forms.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Bryce Kisler, Director
Louis Lee, Audit Manager
Hung Dam, Lead Auditor
Benjamin Bryant, Senior Auditor
Charlene Elliston, Senior Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Deputy Chief Information Officer for Operations
Chief Information Officer
Associate Chief Information Officer, Applications Development
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Director, Office of Audit Coordination

Appendix IV

Glossary of Terms

Term	Definition
Application	A software program hosted by an information system.
Computer Security Incident Response Center	Part of the IRS's Information Technology Cybersecurity organization. The Computer Security Incident Response Center'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 cyberattacks. One of its primary duties is to perform 24-hour monitoring and support to IRS operations.
Contingency Planning	The process of developing advanced arrangements and procedures that enable an organization to respond to an undesired event that negatively affects the organization.
Continuous Diagnostics and Mitigation	A dynamic approach to strengthening Government networks and systems. Led by the Department of Homeland Security, it provides Federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.
Customer Account Data Engine 2	Establishes a single database that houses all individual taxpayer accounts, including IMF data, which provides IRS employees the ability to view updated account information online.
Data Breach	An incident in which sensitive, protected, or confidential data have potentially been viewed, stolen, or used by an individual unauthorized to do so.
Disaster Recovery Server	A server dedicated to testing the ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.
Exposed Administrative Interface	Can enable an unauthorized user to access management and administrative functions of the device or application. This type of access is typically restricted and usually does not include additional layers of access control. An attacker can conduct a brute force attack against an administrative interface that places no restrictions on login attempts.
Firmware Component	The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.
FISMA Master Inventory	A record of IRS general support systems, major applications, and other applications as defined by FISMA guidelines.
FISMA System/Application	Systems or applications included in the FISMA Master Inventory.
Hardware Component	The physical components of an information system.

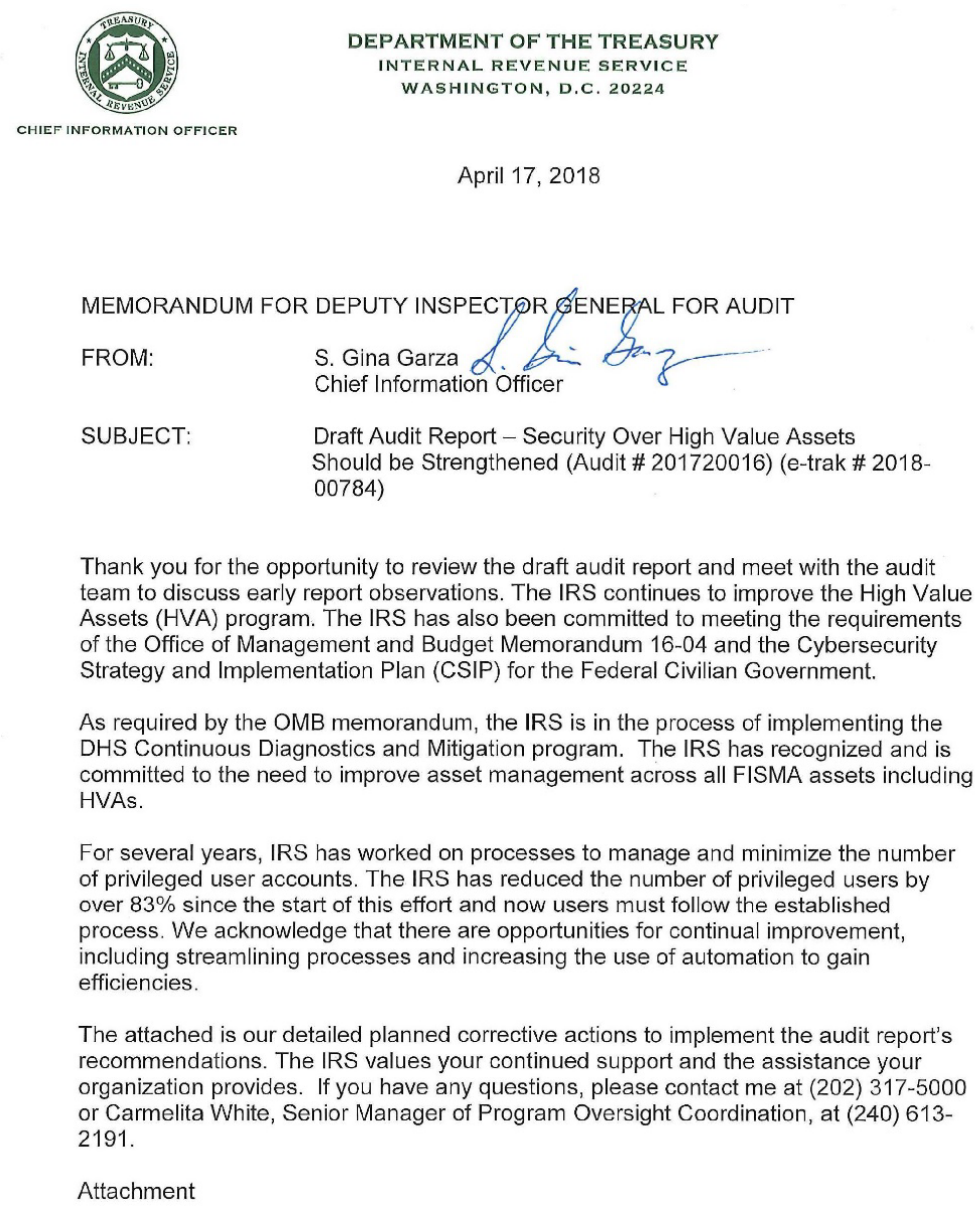
Term	Definition
High Value Assets	Refers to those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions, or data used in critical Federal operations or house unique collections of data (by size or content) making them of particular interest to criminal, politically-motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government.
Individual Master File	The IRS database that maintains transactions or records of individual tax accounts.
Integrated Data Retrieval System	A major application that is a mission-critical system consisting of databases and operating programs that support IRS employees working active tax cases within each business function across the entire IRS. This system manages data that have been retrieved from the Master File, allowing IRS employees to take specific actions on taxpayer account issues, track statuses, and post transaction updates back to the Master File. It provides for systemic review of case status and notice issuance based on case criteria, alleviating staffing needs and providing consistency in case control. The IDRS processes live taxpayer data.
Internal Revenue Manual	The IRS's primary source of instructions to its employees relating to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
Internet Protocol Address	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.
Linux	A free and open-sourced computer operating system. Various distributors (*e.g.*, Red Hat) charge for customized versions of Linux and to support Linux.
Microsoft Windows 2003	A version of Microsoft Windows computer operating systems. It was released in Calendar Year 2003, and Microsoft ended its extended support for the server version of this operating system on July 14, 2015.
Middleware Component	Software that functions at an intermediate layer between applications and operating system or database management system or between client and server.
Online 5081 System	A web-based application that allows users to request access, modify existing accounts, reset passwords, and request deletion of accounts when access is no longer needed to specific systems. The application also allows the IRS to track user access history, generate reports, and document an audit trail of user actions.
Partitioned Server	A reserved part of a storage drive (*e.g.*, server) that is treated as a separate server.
Patch	An update to an operating system, application, or other software issued specifically to correct particular problems with the software.
Penetration Testing	A test methodology in which assessors, using all available documentation (*e.g.*, system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

Term	Definition
Personally Identifiable Information	Information that, either alone or in combination with other information, can be used to uniquely identify an individual. Some examples of Personally Identifiable Information are: name, Social Security Number, date of birth, place of birth, address, and biometric record.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Privilege	A right granted to an individual, a program, or a process.
Privileged Access/Account/User	Any user right assignment that is above the organization's baseline for regular users. Sometimes referred to as system or network administrative accounts.
Risk Vulnerability Assessment	A process that defines, identifies, and classifies the security holes (*i.e.*, vulnerabilities) in a computer, network, or communications infrastructure. In addition, risk vulnerability assessments can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.
Security Breach	Any incident that results in unauthorized access of data, applications, services, networks, or devices by bypassing their underlying security mechanisms. A security breach is also known as a security violation.
Security Controls Assessment	The testing and evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Patch	A fix to a program that eliminates a vulnerability exploited by malicious hackers.
Server	A physical computer (a computer hardware system) dedicated to running one or more services (as a host) to serve the needs of the users of other computers on the network. Depending on the computing service that it offers, it could be a database server, file server, mail server, print server, web server, gaming server, or some other kind of server.
Session	The period of time a user interfaces with an application. The user session begins when the user accesses the application and ends when the user quits the application.
Severity Rating	One of five levels on a ratings scale to describe the risk associated with a vulnerability. The complete scale from lowest risk to highest risk is: Informational, Low, Medium, High, and Critical.
SharePoint Investment Knowledge Exchange System	A Treasury Department capital planning portfolio management tool used to generate data for the Capital Investment Plan and the Summary of Capital Investments.
Spear Phishing	Attacks that use custom-tailored e-mail messages embedded with links or files designed to entice a user to visit a malicious website or download a malicious file, usually resulting in a malware infection or other compromise of the remote host.

Term	Definition
Sprint	A set period of time during which specific work has to be completed and made ready for review.
Standard Operating Procedures	A set of step-by-step instructions compiled by an organization to help workers carry out complex routine operations.
System Boundary	The physical or logical perimeter of a system.
System Security Plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Systems Development Server	A server dedicated in the process of defining, testing, and implementing a new software application or program.
Testing Server	A server that is used on a system under test to verify that the system performs as expected.
Tier I Environment	A computing infrastructure consisting of mainframe computers that handle a high volume of critical operational data.
Tier II Environment	A computing infrastructure consisting of non-mainframe servers. These servers run various operating systems. The servers may also operate as database, web, e-mail, and file servers and provide a host of other important functions supporting the IRS network infrastructure.
Treasury FISMA Inventory Management System	It is the official FISMA data repository for all Treasury Department bureaus. The data maintained in this repository are used as part of the Treasury Department's efforts to comply with the E-Government Act of 2002 (Pub. L. 107-347, 116 Stat. 2899) as well as National Institute of Standards and Technology and OMB regulations and guidance.
Virtual Server	A simulated environment created by virtualization, also described as a tightly isolated software container that can run its own operating systems and applications as if it were a physical computer.
Vulnerability	A flaw or weakness in an information system's design, implementation, or operation and management that could potentially be exploited by a threat to gain unauthorized access to information, disrupt critical processing, or otherwise violate the system's security policy.
Vulnerability Metric	A way to measure weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.
Vulnerability Scanning	The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited or threatened. Employs software that seeks out security flaws based on a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that an individual or an enterprise can use to tighten the network's security.

Appendix V

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CHIEF INFORMATION OFFICER

April 17, 2018

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
Chief Information Officer

SUBJECT: Draft Audit Report – Security Over High Value Assets Should be Strengthened (Audit # 201720016) (e-trak # 2018-00784)

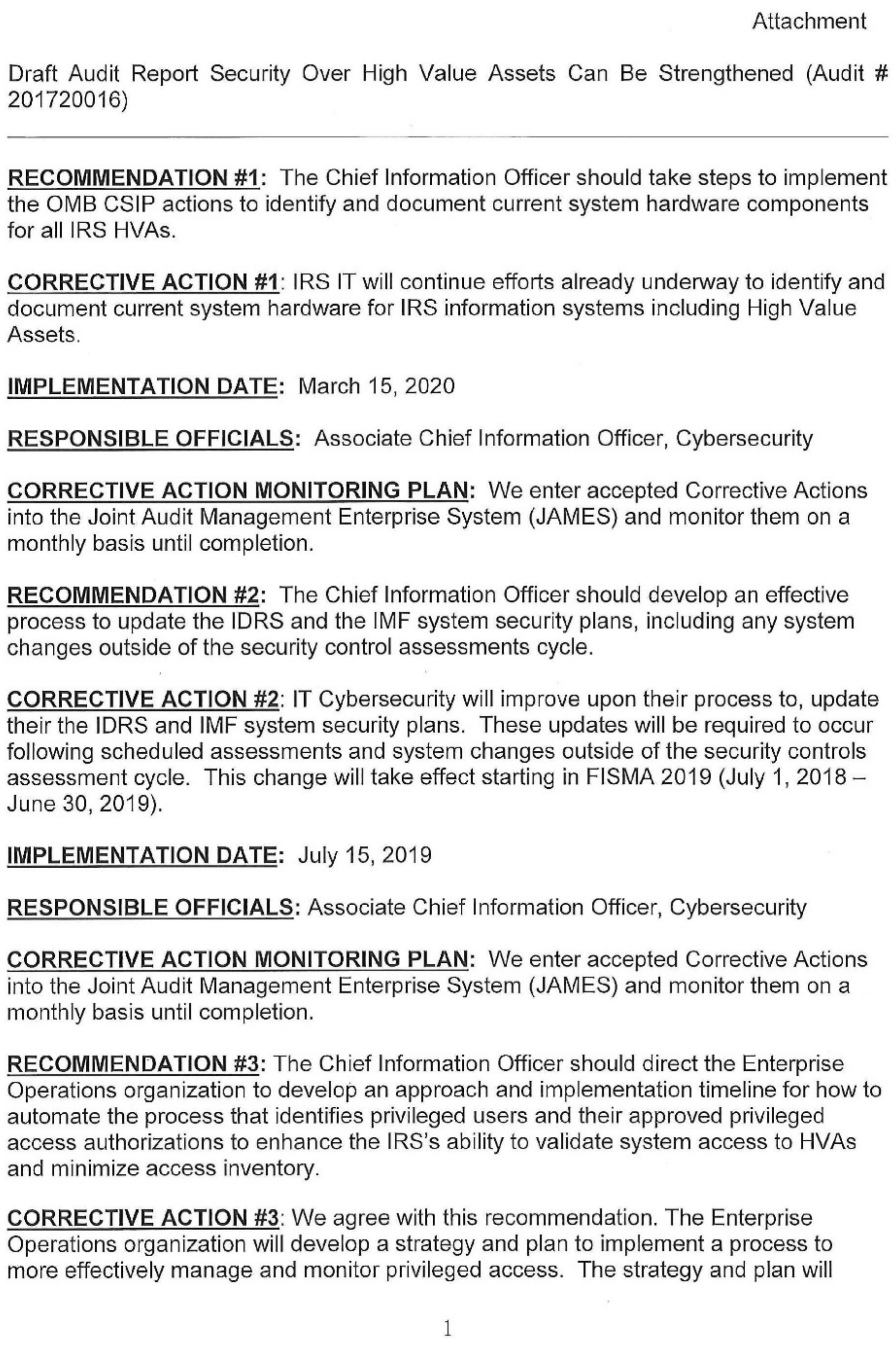
Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss early report observations. The IRS continues to improve the High Value Assets (HVA) program. The IRS has also been committed to meeting the requirements of the Office of Management and Budget Memorandum 16-04 and the Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government.

As required by the OMB memorandum, the IRS is in the process of implementing the DHS Continuous Diagnostics and Mitigation program. The IRS has recognized and is committed to the need to improve asset management across all FISMA assets including HVAs.

For several years, IRS has worked on processes to manage and minimize the number of privileged user accounts. The IRS has reduced the number of privileged users by over 83% since the start of this effort and now users must follow the established process. We acknowledge that there are opportunities for continual improvement, including streamlining processes and increasing the use of automation to gain efficiencies.

The attached is our detailed planned corrective actions to implement the audit report's recommendations. The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 317-5000 or Carmelita White, Senior Manager of Program Oversight Coordination, at (240) 613-2191.

Attachment



Attachment

Draft Audit Report Security Over High Value Assets Can Be Strengthened (Audit # 201720016)

RECOMMENDATION #1: The Chief Information Officer should take steps to implement the OMB CSIP actions to identify and document current system hardware components for all IRS HVAs.

CORRECTIVE ACTION #1: IRS IT will continue efforts already underway to identify and document current system hardware for IRS information systems including High Value Assets.

IMPLEMENTATION DATE: March 15, 2020

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Chief Information Officer should develop an effective process to update the IDRS and the IMF system security plans, including any system changes outside of the security control assessments cycle.

CORRECTIVE ACTION #2: IT Cybersecurity will improve upon their process to, update their the IDRS and IMF system security plans. These updates will be required to occur following scheduled assessments and system changes outside of the security controls assessment cycle. This change will take effect starting in FISMA 2019 (July 1, 2018 – June 30, 2019).

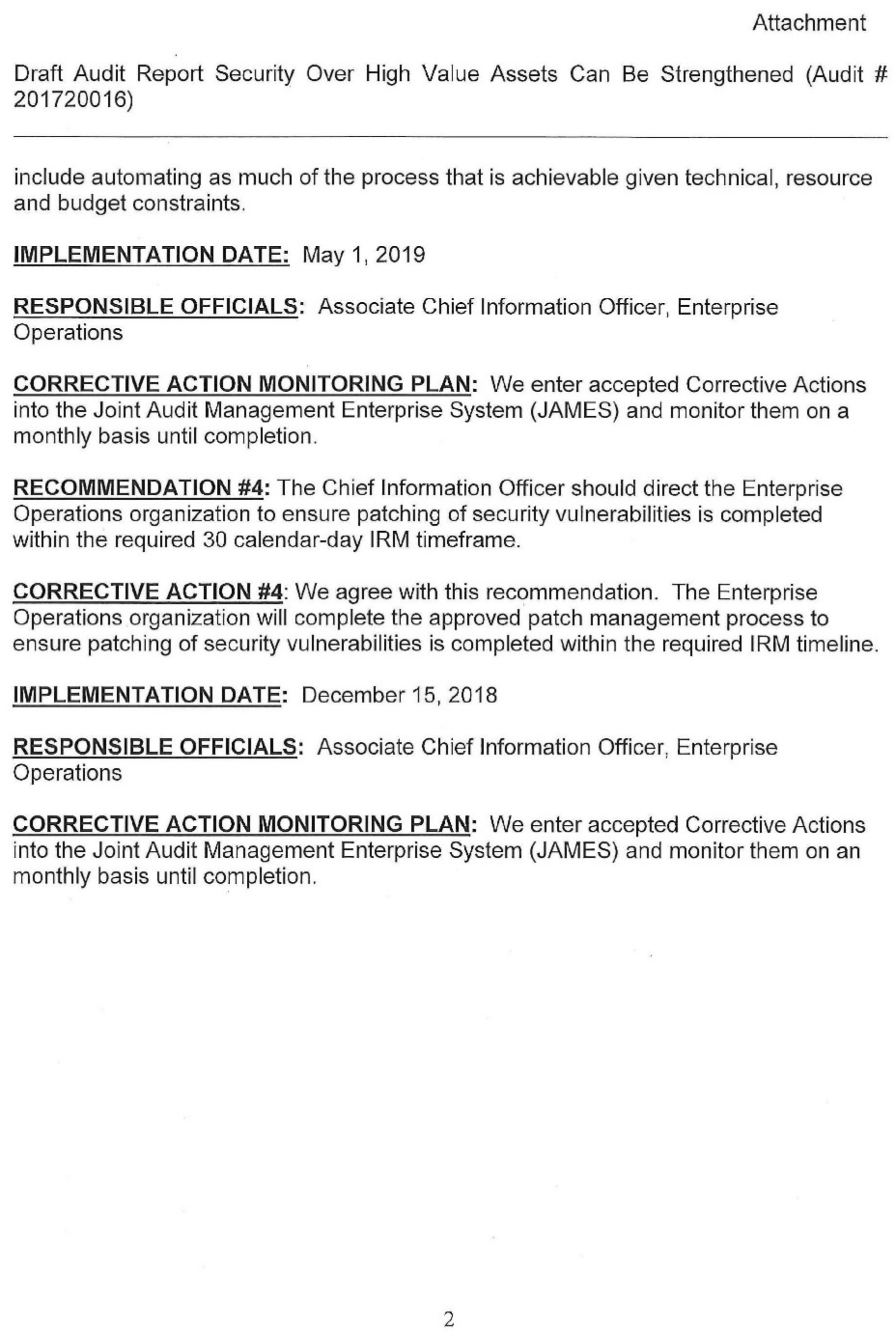
IMPLEMENTATION DATE: July 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #3: The Chief Information Officer should direct the Enterprise Operations organization to develop an approach and implementation timeline for how to automate the process that identifies privileged users and their approved privileged access authorizations to enhance the IRS's ability to validate system access to HVAs and minimize access inventory.

CORRECTIVE ACTION #3: We agree with this recommendation. The Enterprise Operations organization will develop a strategy and plan to implement a process to more effectively manage and monitor privileged access. The strategy and plan will



Attachment

Draft Audit Report Security Over High Value Assets Can Be Strengthened (Audit # 201720016)

include automating as much of the process that is achievable given technical, resource and budget constraints.

IMPLEMENTATION DATE: May 1, 2019

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #4: The Chief Information Officer should direct the Enterprise Operations organization to ensure patching of security vulnerabilities is completed within the required 30 calendar-day IRM timeframe.

CORRECTIVE ACTION #4: We agree with this recommendation. The Enterprise Operations organization will complete the approved patch management process to ensure patching of security vulnerabilities is completed within the required IRM timeline.

IMPLEMENTATION DATE: December 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on an monthly basis until completion.