TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Firewall Administration Needs Improvement

September 24, 2019

Reference Number: 2019-20-061

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:
11 = Disclosure of the Information is Prohibited by Statute or Federal Regulation

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.

FIREWALL ADMINISTRATION NEEDS IMPROVEMENT

Highlights

Final Report issued on September 24, 2019

Highlights of Reference Number: 2019-20-061 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

Firewalls are devices or programs that monitor incoming and outgoing network traffic. An organization's firewall environment acts as a barrier between a trusted network and an untrusted network. Without proper firewall security controls, there is an increased risk of unauthorized access to the IRS ******11******** ***11*** boundary that could result in the loss of sensitive taxpayer data.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether the firewall environment is being administered effectively to protect internal networks from external threats.

WHAT TIGTA FOUND

The IRS is meeting minimum firewall administration requirements, but improvements are required in the following areas: firewall change requests, annual reviews of firewall rulesets, review of firewall system administrator accounts, and password expiration configuration settings.

Required annual reviews of firewall rulesets for the ********11******** boundary are not being performed. TIGTA reviewed ***11*** firewall rulesets for the ********11******** boundary and found extraneous rules. In addition, five firewall change requests associated with four firewall rulesets were implemented without proper approvals authorizing deployment in the ********11******** boundary.

An analysis of firewall system administrator accounts identified one unauthorized account. Additional analysis of login activity reports showed that this account accessed the ********11******** firewalls on three occasions without proper authorization. However, TIGTA determined that the administrator's actions were valid for his or her role and responsibilities. In addition, some password settings for firewall administrator accounts were not set to expire, as required.

Furthermore, firewall inventories and monthly Treasury Cybersecurity Analysis and Reporting Dashboard reports were inaccurate and incomplete, and none of the ********11******** firewalls were correctly categorized in the appropriate information technology asset grouping.

WHAT TIGTA RECOMMENDED

TIGTA made a total of 10 recommendations, which included that the Chief Information Officer and the Chief, Criminal Investigation, ensure that annual reviews of all firewall rulesets are completed, agency policies and procedures are updated to ensure that all firewall change requests and firewall rulesets are assigned appropriate expiration dates, and enforce current request and approval policy for all firewall administrator accounts to ensure that these accounts are compliant with authorization requirements.

In addition, TIGTA recommended that the Chief Information Officer and the Chief, Criminal Investigation, ensure that comprehensive and accurate inventories of information system components are maintained, that appropriate personnel obtain write access within the official enterprise inventory system, and that data field accuracy in the firewall inventories are improved.

The IRS agreed with nine recommendations and partially agreed with one recommendation. The IRS plans to designate expiration dates, conduct annual reviews of all rulesets, conduct periodic audits of administrative accounts, and conduct periodic reviews of asset inventories. The IRS partially agreed with the recommendation for improving and updating asset inventory records and proposed an alternative remediation to accomplish the intent of the recommendation.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 24, 2019

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Firewall Administration Needs Improvement (Audit # 201920014)

This report presents the results of our review of Internal Revenue Service (IRS) firewall administration to determine whether the firewall environment is administered effectively to protect internal networks from external threats. This audit is included in our Fiscal Year 2019 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

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

Copies of this report are also being sent to the IRS 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

CARD	Cybersecurity Analysis and Reporting Dashboard
CI	Criminal Investigation
11	***********11**********
FCR	Firewall Change Request
FISMA	Federal Information Security Modernization Act of 2014
GSS	General Support System
11	***********11**********
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
UNS	User and Network Services

Background

Firewalls are devices or programs that monitor incoming and outgoing network traffic and decide whether to allow or block specific traffic based on a defined set of security rules.[1] An organization's firewall environment acts as a barrier between a trusted network and an untrusted network, *e.g.*, the Internet. Effective firewall administration is paramount to ensure that unwanted traffic does not pass through and infiltrate the internal network.

According to the National Institute of Standards and Technology (NIST),[2] organizations should implement the following recommendations to improve the effectiveness and security of their firewalls:

- Create a firewall policy that specifies how firewalls should handle inbound and outbound network traffic. A firewall policy defines how firewalls should handle inbound and outbound network traffic for specific Internet Protocol addresses and address ranges, protocols, applications, and content types based on the organization's information security policies.
- Create rulesets that implement the organization's firewall policy while supporting firewall performance. Firewall rulesets should be as specific as possible about the network traffic they control.
- Manage firewall architectures, policies, software, and other components throughout the life of the firewall solutions. There are many aspects to firewall management. For example, policy rules may need to be updated as requirements change, such as when new applications are implemented within the network.

The Internal Revenue Manual (IRM)[3] states that the Computer Security Incident Response Center shall establish and manage the Minimum Firewall Administration Requirements as well as oversee and approve all rulesets for the Internal Revenue Service (IRS) network perimeter firewall environments. In conjunction with the Computer Security Incident Response Center, the User and Network Services (UNS) function's Engineering office shall design the network perimeter demilitarized zones, including firewall requirements, and shall be responsible for firewall implementation and maintenance.

[1] See Appendix V for a glossary of terms.
[2] NIST 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy* (Sept. 2009).
[3] IRM 10.8.54, *Information Technology Security, Minimum Firewall Administration Requirements* (Nov. 15, 2018).

Currently, the IRS has *11* Federal Information Security Modernization Act of 2014 (FISMA)[4] reportable firewalls at the IRS campuses ********************11***********************
***************************************11*************************************
*******11*******. According to the FISMA, General Support Systems (GSS) are "reportable" systems. The Office of Management and Budget[5] defines GSS as an interconnected set of information resources under the same direct management control that shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. Each of the **11** firewalls are located within the following two IRS GSSs:

- GSS-1 **************************11***************************************
  ********************************11***************************************
  ********************************11***************************************
  ********************************11***************************************
  ********************************11***.
- Criminal Investigation (CI)-2 ********11**************************************
  ********************************11***************************************
  ********************************11***************************************
  ********************************11***************************************
  ********************************11***************************************
  11,[6] ****11*****.

[4] Pub. L. No. 113-283, 128 Stat. 3703. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

[5] Appendix III of Office of Management and Budget, Circular No. A-130 (Revised), *Security of Federal Automated Information Resources* (July 27, 2016).

[6] *11* GSS-1 ************************************11**.

***************************************11**********************************

*****11*****	***11*** ***11***	***11*** ***11***	***11*** ***11***	***11*** ***11***	**11**
*****11********* *****11*****	*11*	*11*	*11*	*11*	*11*
*****11*******	*11*	*11*	*11*	*11*	*11*
*****11*******	*11*	*11*	*11*	*11*	*11*
*****11********* *****11*****	*11*	*11*	*11*	*11*	*11*
*****11********* *****11*****	*11*	*11*	*11*	*11*	*11*
*****11********* *****11*****	*11*	*11*	*11*	*11*	*11*
*****11*******	*11*	*11*	*11*	*11*	*11*
*****11*******	*11*	*11*	*11*	*11*	*11*
*****11********* *****11*****	*11*	*11*	*11*	*11*	*11*
*****11********* *****11*****	*11*	*11*	*11*	*11*	*11*
11	*11*	*11*	*11*	*11*	*11*
11	*11*	*11*	*11*	*11*	*11*

11*
*******************11***************.

This review was performed during the period November 2018 through July 2019 *****11***** **************************************11************************************ **************************************11*****************. We worked closely with CI, and the Information Technology organization's UNS and Cybersecurity functions. 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 findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors are listed in Appendix II.

Results of Review

Minimum Firewall Administration Requirements Are Being Met, but Administrative Oversight and Required Reviews Are Inconsistent

The IRM states that the minimum firewall administration requirements at the IRS are guided by three fundamental objectives:

- To ensure that no traffic is admitted into or out of IRS protected networks unless it is expressly permitted.
- The perimeter firewall environments are installed so that all traffic between IRS protected networks and the outside must pass through these firewall environments.
- All traffic between systems in a security zone and the intranet shall traverse a firewall, including all systems administration traffic, portal application traffic, and backup system traffic.

While we determined that both the GSS-1 and the CI-2 are meeting minimum firewall administration requirements, improvements are needed to ensure that the firewalls continue to protect IRS internal networks from external threats. To reduce these risks, the IRS needs to make improvements to the Firewall Change Request (FCR) process, implement annual reviews of all firewall rulesets and user accounts, and enforce password expiration requirements.

Annual firewall ruleset review

The required GSS-1 annual firewall ruleset reviews are not being performed. We reviewed *11* GSS-1 firewall rulesets and found extraneous rules in the firewalls. Alternately, CI-2 firewall rulesets are being reviewed on an annual basis. We reviewed *11* CI-2 firewall rulesets and did not find extraneous rules in the firewalls.

The NIST requires firewall rulesets and policies to be managed by a formal change management control process because of their potential impact to security and business operations, with ruleset reviews or tests performed periodically to ensure continued compliance with the organization's policies. In addition, the IRM requires an annual review of all firewall rulesets to ensure that they are still necessary and remain in compliance with the security policy, or as new threats are identified and requirements change.

The Computer Security Incident Response Center and the UNS Firewall Support Team stated that the required annual reviews were not completed due to lack of adequate staffing and the absence of a network security management appliance with the ability to perform automated reviews. In February 2019, the UNS Firewall Support Team completed an initial manual review of all *11* GSS-1 firewall rulesets associated with all *********11************* firewalls. The results of the review showed that *11* (39 percent) of the GSS-1 rulesets were not used within the previous 90 days. In addition, the UNS Firewall Support Team is testing a new network security management appliance that will allow for automated reviews and testing of all firewall rulesets. The UNS Firewall Support team stated that it planned for the new network security management appliance to be implemented prior to the 2020 Filing Season.

As a result of not performing required annual firewall ruleset reviews, there is an increased risk of unauthorized access to the *******11******** boundary that could result in the loss of sensitive taxpayer data.

Firewall change requests

We reviewed all 164 FCRs associated with current GSS-1 and CI-2 firewall rulesets. We found that all 11 of the CI-2's FCRs were properly approved and correctly implemented. Of the 153 GSS-1 FCRs, we determined that five (3 percent) FCRs associated with four rulesets were implemented without approvals authorizing deployment in the GSS-1 firewall environment.

The IRM states that a log of all policy decisions and ruleset changes shall be kept and associated with the firewall; and, whenever practical, rulesets should be documented with comments and an approved FCR reference on each firewall ruleset. Industry best practices recommend setting expiration dates on rulesets to help identify irrelevant rules as soon as possible and remove them to prevent degradation of performance, security, and manageability.

The FCR process uses a form that requires manual data entry. There is no IRS requirement to assign an expiration date to either the FCR or firewall ruleset, however, an adequate network security management appliance would facilitate automated reviews of rulesets and enforce expiration dates.

By not ensuring that all firewall rulesets have an approved FCR and by not implementing expiration dates, there is an increased risk that network traffic flowing through the firewalls is not included in the approved services, protocols, and ports listing. As a result, IRS networks are potentially exposed to unnecessary and unmanaged risk.

Unauthorized administrator account

We also reviewed *11* GSS-1 and *11* CI-2 firewall system administrator accounts and identified one GSS-1 account that was not authorized through the Online 5081 application. In addition, we reviewed login activity reports that showed that this system administrator accessed the GSS-1 firewalls on three occasions without proper authorization. However, we determined the administrator's actions were valid for his or her role and responsibilities. We notified the UNS Firewall Support Team and they took corrective action to ensure that the Online 5081 authorization was completed.

The NIST[7] requires valid access authorization for access to information systems and accounts be reviewed for agency compliance with account management requirements. Agency policies require approval by the system owner for requests, via the Online 5081 application, to create system accounts. In addition, privileged accounts shall be reviewed semi-annually for compliance with account management requirements. Privileged accounts include system administrators for the various types of operating systems.

The UNS Firewall Support Team did not ensure that GSS-1 administrator accounts were compliant with agency requirements for granting system access and did not review firewall administrator accounts semi-annually. Improper account management increases the risk of an unauthorized user gaining access to sensitive and privileged data within the information systems.

Firewall password expiration

We reviewed password expiration configuration settings for the GSS-1 and CI-2 firewalls. We found no issues with the GSS-1 firewalls; however, the CI-2 firewall password settings were not configured to enforce password expiration. The IRM requires a maximum password age or expiration for application and operating systems to be set at 90 days.

CI management officials told us that local firewall administrator accounts did not include password expiration to ensure that the administrators do not get locked out. In addition, the accounts cannot be unlocked remotely and personnel resources are not located on site.

During our review, CI management officials initiated a corrective action to remove all local firewall administrator accounts and configure all the CI-2 firewalls to use an authentication protocol authorizing access to the firewalls. This action should ensure compliance with the IRM's maximum password age requirements for users and administrators.

Failure to properly manage passwords could result in unauthorized access to information systems, which could compromise the confidentiality, integrity, and availability of the system.

Recommendations

The Chief Information Officer and the Chief, CI, should:

Recommendation 1: Conduct annual reviews of all firewall rulesets in accordance with agency policies and procedures.

> ***Management's Response:*** The IRS agreed with this recommendation and will conduct annual reviews of all firewall rulesets in accordance with agency policies and procedures.

[7] NIST Special Publication 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* (Dec. 2014).

Recommendation 2**:** Assign expiration dates not to exceed 365 days to firewall policies.

Management's Response: The IRS agreed with this recommendation and will assign designated expiration dates to firewall policies.

Recommendation 3: Conduct periodic firewall administrator account audits in accordance with agency policies and procedures.

Management's Response: The IRS agreed with this recommendation and will conduct periodic audits of firewall administrator accounts in accordance with agency policies and procedures.

Recommendation 4: Ensure that all firewall password settings are configured to expire in accordance with agency policies.

Management's Response: The IRS agreed with this recommendation. Following audit fieldwork, CI officials confirmed that all firewall password settings were configured in accordance with agency policies.

Firewall Inventory and Reporting Tools Are Inaccurate and Incomplete

The IRS utilizes multiple inventory and reporting tools to assist in providing administrative oversight of all FISMA reportable firewalls. We reviewed multiple **********11*********** ***11*** firewall inventory reports and the Department of the Treasury (hereafter referred to as Treasury Department) Cybersecurity Analysis and Reporting Dashboard (CARD) monthly inputs.[8] Figure 2 provides a summary of the total FISMA reportable firewalls using the various inventory and reporting tools, and compares it to the correct number of firewalls in the inventory.

[8] There is no monthly reporting requirement for the *******11******* inventory. We requested an ***11*** ***11*** inventory report for the same months as the Treasury CARD reports.

****************************11**************************
**************************11**************************

******11******	***11*** ***11*** ****11****	***11*** ***11*** ****11****	***11*** ***11*** ****11****	***11*** ***11*** ****11****	****11**** ***11*** ***11***
11* ***11**** ***11****	*11*	*11*	*11*	*11*	*11*
11* ***11**** ***11****	*11*	*11*	*11*	*11*	*11*
11* ***11**** ***11****	*11*	*11*	*11*	*11*	*11*

11************************************
******************11*************.

We determined that each of the firewall inventory and reporting tools were not only inaccurate and incomplete, but also reported conflicting numbers of FISMA reportable firewalls.

**************11************ firewall inventories

During our review, we evaluated the *******11******* inventory specific to the GSS-1 and CI-2 firewalls. *******11******* is a component of the Knowledge, Incident/Problem Service Asset Management system, which is the official financial asset inventory system. We determined that the November 2018, February 2019, and April 2019 inventory reports were both inaccurate and incomplete and did not contain the level of granularity required for timely and up-to-date tracking and reporting of IRS firewalls. However, throughout the course of the audit, the UNS function's Asset Management program completed multiple updates to the GSS-1 and CI-2 firewall inventories. As a result, the May 2019 ******11****** GSS-1 and CI-2 firewall inventories provided an accurate and current snapshot.

Additional examples of inaccurate and incomplete reporting include:

- In the November 2018, and February 2019 inventory reports, two firewalls were documented as residing in *********11*********. However, Treasury Inspector General for Tax Administration auditors verified that both firewalls are located in the ******11******.
- In the November 2018 and February 2019 inventory reports, multiple data fields were not populated with current data.

- In the November 2018, February 2019, and April 2019 inventory reports, one GSS-1 firewall was listed as *In Stock*. However, Treasury Inspector General for Tax Administration auditors verified that the firewall is *In Use* *********11*********.
- In the November 2018, February 2019, and April 2019 inventory reports, nine **11** *11* CI-2 firewalls were incorrectly categorized as *Appliances* or *Gateways*.
- In the November 2018 and February 2019 inventory reports, 38 percent of the GSS-1 firewalls did not contain an *********11*********. This data field is designed to receive input via an automated module; however, the process of automating the **11** ******11****** data field is inconsistently applied.

The IRM[9] requires system owners to develop and document an inventory of information system components that is accurate, includes all components within the authorization boundary of the information system, captures both hardware and software, and with the level of granularity deemed necessary for tracking and reporting.

The IRS maintains inventory records for its trackable components in its ******11****** inventory system. The inventory system relies heavily on manual data entry and does not sufficiently leverage available automated tools to assist in maintaining an up-to-date, complete, and accurate inventory. Due to the ******11****** inventory system's reliance on manual processes, initial records for new firewalls took up to eight months to appear in inventory records. In addition, routine inventory updates took between four to eight weeks to appear in inventory records. In one example, between September and October 2018 the IRS received *11* new firewalls that were operational within two to three months, however, these firewalls were not added to the inventory until May 2019.

The UNS Firewall Support Team and CI Inventory Specialists stated that one of the primary reasons for the lack of timely and accurate inventory reporting is due to local Inventory Specialists not having write access to key data fields. At the end of our fieldwork, the UNS Asset Management Team told us that there are several methods for reporting inventory transactional updates to ******11******.[10]

Without accurate GSS-1 and CI-2 firewall inventories, the IRS cannot ensure that it is properly monitoring and maintaining perimeter supporting components in a secure manner.

Treasury Cybersecurity Analysis and Reporting Dashboard

From July 2017 through February 2019, the IRS's monthly submission for the Treasury Department's CARD reported the same incorrect number of firewalls *11* connected to

[9] IRM 10.8.1, *Information Technology Security, Policy and Guidance* (May 9, 2019).
[10] The Treasury Inspector General for Tax Administration did not evaluate these methods to determine if they would improve the accuracy and timeliness of the firewall inventory.

unclassified networks. The Cybersecurity function's Office of Strategy and Business Analytics is responsible for all facets of the monthly Treasury Department CARD submission. This includes requesting and consolidating data inputs from key stakeholders and subject matter experts, reviewing inputs for possible errors and anomalies, and submission of the final report to the Treasury Department. The Office of Strategy and Business Analytics officials stated that the number reported should include all FISMA reportable firewalls. As previously illustrated in Figure 1, the IRS employs *11* FISMA reportable firewalls that are connected to unclassified networks.

The FISMA directs Federal agencies to report annually to the Office of Management and Budget Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices, and compliance with the FISMA. In addition to the annual FISMA reporting requirements, the Office of Management and Budget also directs Federal agencies to report monthly on key information security metrics.

We found that key management stakeholders and subject matter experts responsible for the GSS-1 and CI-2 were unaware of the Treasury Department's CARD requirements and thus were not involved in the monthly submission process. However, once we alerted the Office of Strategy and Business Analytics of this issue, the office took corrective action and updated the list of key management stakeholders and subject matter experts responsible for the firewall portion of the Treasury CARD. Without accurate firewall reporting, senior IRS leadership and executive stakeholders may not have accurate information for decision-making.

Information technology asset grouping

The initial GSS-1 security vulnerability reports did not contain results for any of the GSS-1 firewalls because their Internet Protocol addresses were not correctly categorized as belonging to the GSS-1 information technology asset grouping.

The Enterprise Vulnerability Scanning Standard Operating Procedures[11] require the Enterprise Vulnerability Scanning team in the Cybersecurity function to create and maintain information technology asset groupings based on information from the UNS or self-identified inventories via scan request forms submitted by system owners. The team will also determine and vet the set of hardware equipment, operating systems, and software applications that they are capable of scanning.

At the Enterprise Vulnerability Scanning team's request, we provided a complete listing of each of the Internet Protocol addresses for the GSS-1 firewalls. The team subsequently provided vulnerability scans for each of the *11* GSS-1 firewalls. In addition, the Enterprise Vulnerability Scanning team took management action and coordinated with the UNS Firewall Support Team to

[11] IRS, *Enterprise Vulnerability Scanning Standard Operating Procedures, Version 1.3* (Mar. 20, 2018).

submit an updated scan request form, which categorizes the GSS-1 firewalls into the appropriate information technology asset grouping.

Without performing and ensuring accurate information technology asset group listings, there is a risk that unknown or undetected security vulnerabilities could compromise the network security perimeter and potentially lead to unauthorized access, unauthorized data sharing, and unauthorized data exploitation.

Recommendations

The Chief Information Officer and the Chief, CI, should:

Recommendation 5: Ensure that comprehensive and accurate inventories of information system components are maintained, including the GSS-1 and CI-2 inventories, that include the level of granularity necessary for tracking and reporting, and implement improved procedures for ensuring that the inventories remain accurate and up-to-date.

> **Management's Response:** The IRS agreed with this recommendation. The UNS function will conduct, in conjunction with CI, periodic reviews of the GSS-1 and CI-2 firewall asset inventories and update and socialize process guidance on maintaining firewall asset inventories.

Recommendation 6: Ensure that IRS Firewall Support personnel responsible for managing the firewall systems obtain write access to key data fields within ******11****** to improve the efficiency and accuracy of firewall inventory key data fields within ******11******.

> **Management's Response:** The IRS partially agreed with this recommendation. The IRS agreed that the efficiency and accuracy of firewall inventory can be improved. However, the IRS disagreed that the method prescribed in the recommendation to provide write access to key data fields would be the most effective method to improve efficiency and accuracy. To address the finding, the IRS will complete an evaluation to determine the appropriate method for maintaining accuracy and timely updates on firewall asset inventory records and implement a process based on the results of the evaluation.

> **Office of Audit Comment:** We based our recommendation on the existing conditions observed and determined an effective method to improve efficiency and accuracy. We agree that completing an evaluation to determine the appropriate method for maintaining accuracy and timely updates on firewall asset inventory records may provide a more effective method to achieve this goal.

Recommendation 7: Ensure that IRS procedures regarding the monthly Treasury Department CARD input are updated and all FISMA reportable firewalls are reported.

> **Management's Response:** The IRS agreed with this recommendation. Asset owners will remain responsible for accuracy of all reportable asset information. Cybersecurity

will update the CARD Data Collection Matrix with procedures to include validated points of contact, data sources, and FISMA reportable assets.

Recommendation 8: Improve the data field accuracy for the firewall inventories in the *11* *****11*****.

Management's Response: The IRS agreed with this recommendation. As noted during fieldwork, IRS officials took action to update the firewall asset inventory records. To address this finding, the IRS will complete a review of the firewall inventories in *11* *****11***** and process any updates, where identified.

Recommendation 9: Ensure that the Cybersecurity function periodically communicates its Enterprise Vulnerability Scanning Standard Operating Procedures to all relevant stakeholders and follows these procedures and other agency policies to create and maintain information technology asset groupings.

Management's Response: The IRS agreed with this recommendation. Cybersecurity will distribute the Enterprise Vulnerability Scanning Standard Operating Procedures periodically to all relevant stakeholders to ensure stakeholders provide Cybersecurity the information required to create and maintain the information technology asset groupings.

Some Security Vulnerability Scans Were Not Completed

We reviewed security vulnerability scans for the GSS-1 and CI-2 from August 2018 through February 2019 and did not find any issues related to the timely remediation of security vulnerabilities. However, we determined that vulnerability scans were not being performed on *11* (40 percent) of *11*,[12] CI-2 firewalls. The IRM requires that all information systems and applications be scanned for vulnerabilities at a minimum of monthly.

Officials responsible for the CI-2 stated that CI's Technical Operations Center was responsible for the system administration, to include vulnerability scanning for the remaining *11* firewalls. The Technical Operations Center system administrators told us they were unaware of the existence of these two firewalls. During our review, the system administrators commenced the scanning and provided vulnerability reports for the remaining two firewalls.

Failure to perform vulnerability scans can compromise the security posture of the system and can lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing and data exploitation.

[12] *11* of the CI-2's *11* firewalls are in a separate development environment and are not subject to agency security vulnerability scanning requirements.

Recommendation

The Chief Information Officer and the Chief, CI, should:

Recommendation 10: Ensure that all CI information systems comply with agency policies and procedures regarding security vulnerability scanning.

> **Management's Response:** The IRS agreed with this recommendation. During the audit, CI took immediate steps to confirm the vulnerability scanning was established on all CI firewalls, and will ensure compliance with agency policies and procedures regarding security vulnerability scanning by commencing the vulnerability scanning as new devices are operationalized.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective was to review the IRS firewall administration to determine whether the firewall environment is administered effectively to protect internal networks from external threats. To accomplish this objective, we:

I. Evaluated the management and oversight of the firewall architecture and administration.

A. Conducted research and obtained Federal and IRM policies and procedures that govern the management, operation, and maintenance of firewall devices.

B. Interviewed members of the Computer Security Incident Response Center, UNS, and CI to determine roles, responsibilities, and current duties performed by each group.

C. Determined whether oversight is adequate for the primary objectives contained within the firewall policies.

II. Evaluated firewall rulesets to determine whether they met minimum baseline security controls established by Federal guidance, IRS policy, and industry best practices.

A. Obtained and reviewed firewall rulesets.

B. Obtained and reviewed documentation of the annual review of firewall rulesets.

C. Obtained and reviewed a list of user accounts, from Online 5081, UNS, and CI reports, that have access to firewalls to determine whether those accounts were effectively managed.

III. Determined the completeness and accuracy of the information system components inventory for firewall devices.

A. Obtained and reviewed the UNS and CI Standard Operating Procedures for firewall inventory management.

B. Obtained and reviewed *****11***** inventory reports of IRS firewall devices.

C. Assessed the completeness and accuracy of the data fields contained within the IRS firewall inventory.

D. Determined whether the firewall inventory contained the level of granularity necessary for accurate and up to date tracking and reporting.

E. Obtained and reviewed the monthly Treasury Department CARD for network traffic devices.

IV. Evaluated the change management process in place for firewall devices.

A. Obtained and reviewed relevant change management policies and procedures.

B. Obtained and reviewed all the FCRs for both the GSS-1 and the CI-2, and verified that production FCRs were approved.

C. Determined whether completed change requests followed established policies, procedures, and best practices.

D. Verified that production firewall rulesets had an approved FCR.

V. Determined whether effective controls are in place to discover and remediate vulnerabilities and malicious code on IRS firewall devices.

A. Reviewed GSS-1 and CI-2 vulnerability scans completed from August 2018 through February 2019.

B. Determined whether vulnerabilities were adequately and timely remediated.

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: NIST requirements for the administration of firewall security and IRM policies related to firewall administration and inventory procedures. Through interviews with IRS employees and contractors and review of relevant documentation provided by the IRS, we gained an understanding of the policies and procedures related to its firewall architecture to determine whether the firewall environment is administered effectively in order to protect internal networks from external threats. We extrapolated data from IRS systems to evaluate firewall administrative users, firewall rulesets, and firewall change requests. We examined inventory reports developed from the ***11*** ***11*** inventory system and the Treasury Department CARD reports.

Appendix II

Major Contributors to This Report

Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Jena Whitley, Director
Jason McKnight, Audit Manager
Mike Curtis, Lead Auditor
Naomi Koehler, Senior Auditor
Nicholas Reyes, Senior Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief Criminal Investigation
Chief Information Officer
Deputy Chief, Criminal Investigation
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, User and Network Services
Director, Cybersecurity Operations
Director, Network Engineering
Director, Enterprise Audit Management

Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Reliability of Information – Actual; *11* FISMA reportable firewalls were not accurately listed on the February 2019 ******11****** firewall inventory report (see page 7).

Methodology Used to Measure the Reported Benefit:

We reviewed four GSS-1 and CI-2 *******11******* firewall inventory reports. We also conducted site-visits ******************11*********************************** to verify the location, barcode, and serial number of all FISMA reportable firewalls. Our analysis determined that the February 2019 *******11******* firewall inventory report did not include ****11**** FISMA reportable firewalls.

Type and Value of Outcome Measure:

- Reliability of Information – Actual; *11* FISMA reportable firewalls were not listed accurately on the February 2019 Treasury Department CARD report (see page 7).

Methodology Used to Measure the Reported Benefit:

We reviewed four IRS Treasury Department CARD monthly reports. We also conducted site-visits ******************11*********************************** to verify the location, barcode, and serial number of all FISMA reportable firewalls. Our analysis determined that in February 2019 the Treasury Department CARD report included ****11**** FISMA reportable firewalls. This resulted in *11* FISMA reportable firewalls going unreported in that timeframe.

Appendix V

Glossary of Terms

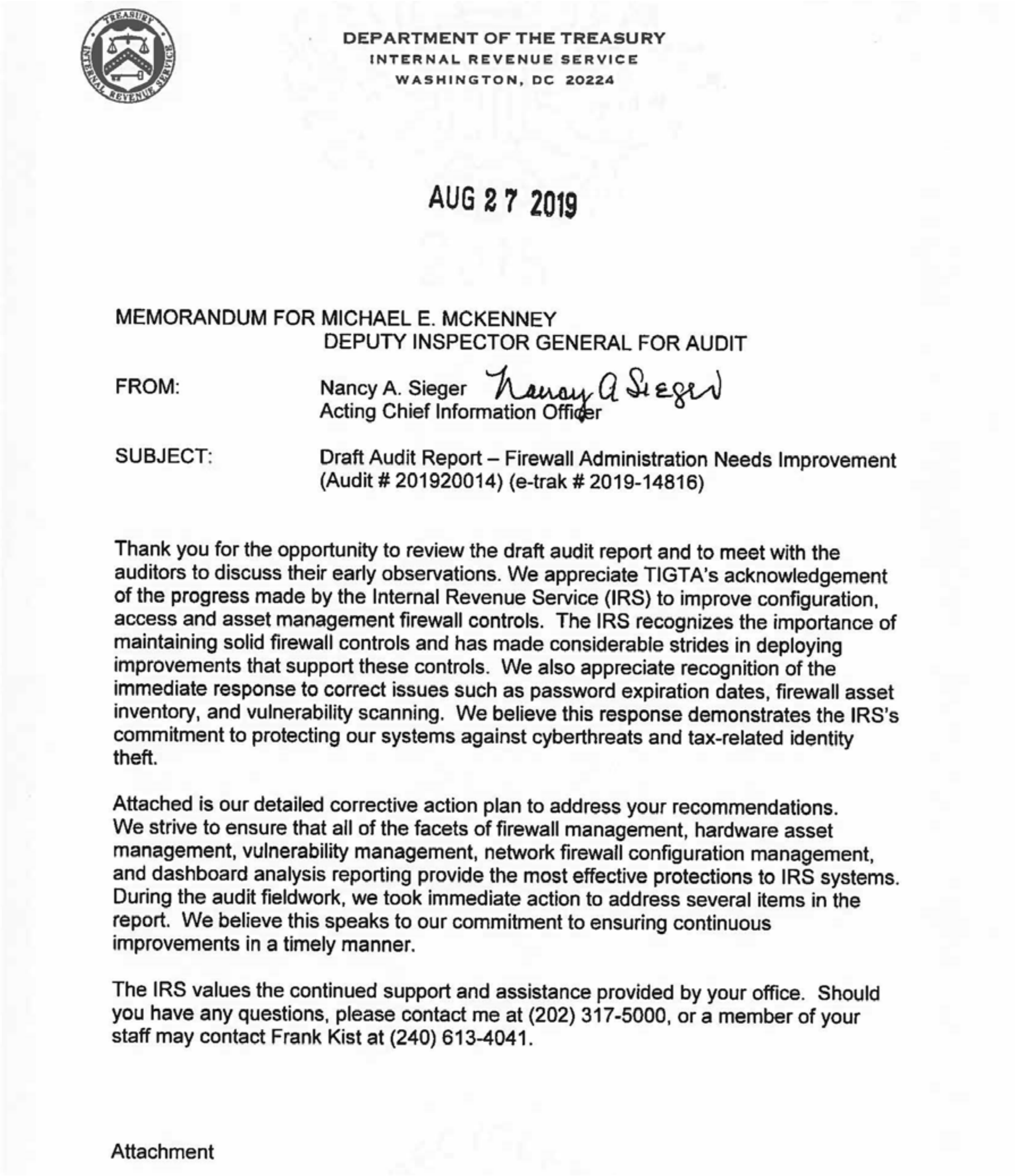
Term	Definition
Availability	Ensuring timely and reliable access to and use of information.
Change Management Control Process	The process responsible for controlling the life cycle of all changes, enabling beneficial changes to be made with minimum disruption to information technology services.
***************11**************	********************************11************************************ ********************************11************************************ ********************************11************************************ ********************************11************************************ ********************************11********.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including a means for protecting personal privacy and proprietary information.
Demilitarized Zone	An unprotected or semi-protected network segment or segments that reside at the perimeter boundary between the trusted intranet and untrusted entities.
*****************11***************** *****11*****	********************************11************************************ ********************************11************************************ ********************************11********.
*****************11***************** *****11*****	********************************11************************************ ********************************11************************************.
***************11**************	********************************11************************************ ********************************11************************************ ********************************11************************************.
Federal Information Security Modernization Act of 2014	Public Law No 113-283, signed into law on December 8, 2014, requires agencies to implement the Director's standards and guidelines for safeguarding Federal information and systems from a known or reasonably suspected information security threat, vulnerability, or risk.
Firewall	A device that has a network protection application installed to safeguard the network from intentional or unintentional intrusion. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet.

Term	Definition
Firewall Change Request	Process to evaluate changes and link actual changes back to the desired outcome.
Firewall Ruleset	A set of instructions that the firewall uses to determine routing and treatment, *e.g.,* allow/deny ports, protocols, and services, for packets being routed between its interfaces.
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.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
***************11**************	********************************11***11***11***11***11***.
***************11**************	********************************11***11*************************************.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Internet Protocol	Standard protocol for the transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
***************11**************	********************************11***11***11***11***11*************************.
Network Security Management Appliance	A device that provides centralized configuration, policy-based provisioning, and updates management and end-to-end network monitoring functionality to enterprise organizations.
Online 5081	A web-based application and is currently the system used to obtain access to needed systems.
System Administrator	An individual employed to maintain and operate the technical aspects of an information system. Usually charged with installing, supporting, and maintaining servers or other computer systems and planning for and responding to service outages and other problems.

Term	Definition
System Security Plan	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.
***************11**************	*******************************11*********************************** *******************************11*********************************** *******************************11*********************************** ***11***.
Trackable Components	Hardware that is barcoded for inventory purposes and includes laptops, desktop computers, servers, and network devices (such as firewalls, routers, and switches).
Trusted Networks	The networks inside an organization's security perimeter.
***************11**************	*******************************11*********************************** *******************************11*********************************** *******************************11*********************************** *******************************11**********************************.
Vulnerability Scan	The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited or threatened. It 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.
***************11**************	*******************************11*********************************** *******************************11*********************************** *************11*************.

Appendix VI

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

AUG 27 2019

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger Nancy A Sieger
Acting Chief Information Officer

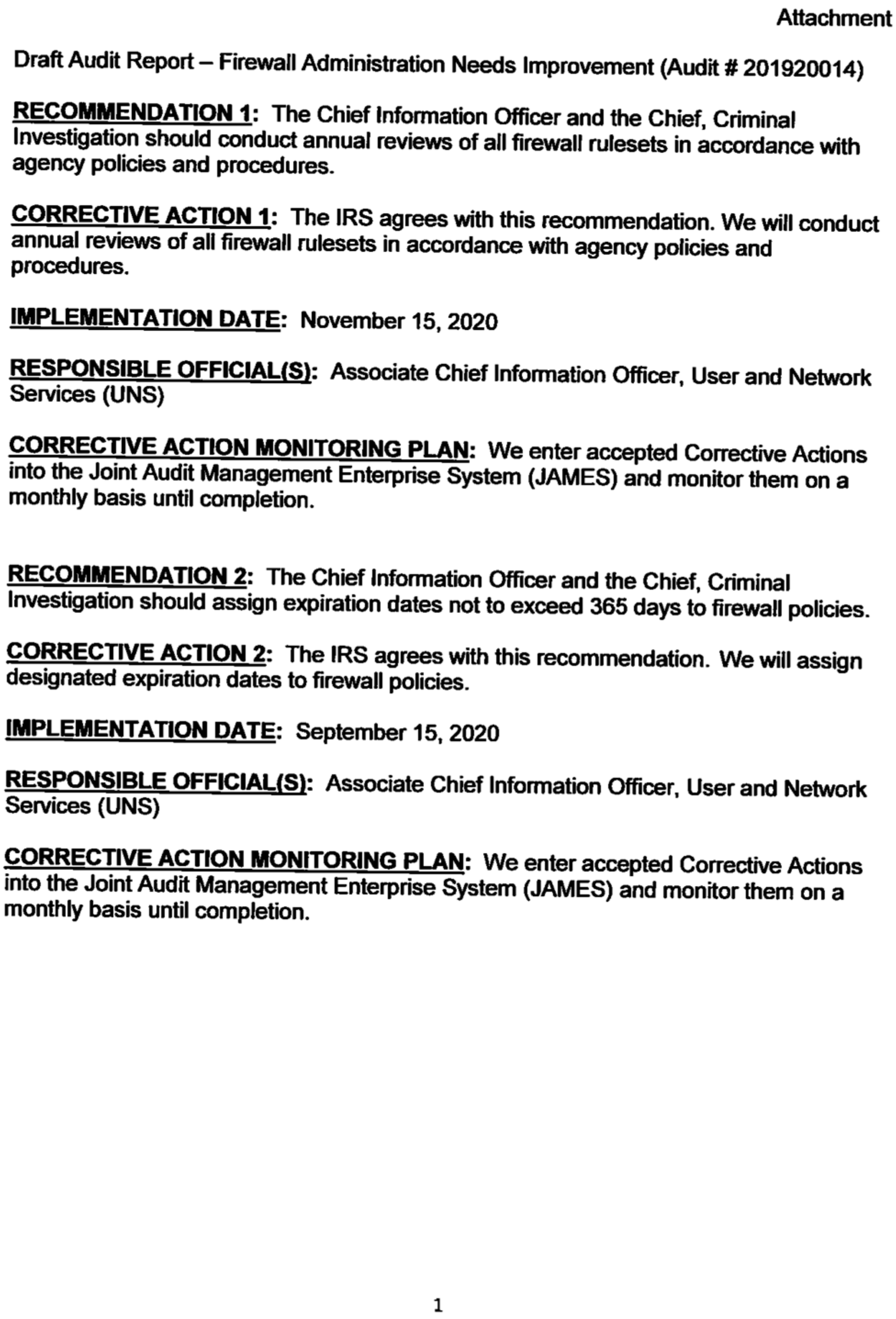
SUBJECT: Draft Audit Report – Firewall Administration Needs Improvement (Audit # 201920014) (e-trak # 2019-14816)

Thank you for the opportunity to review the draft audit report and to meet with the auditors to discuss their early observations. We appreciate TIGTA's acknowledgement of the progress made by the Internal Revenue Service (IRS) to improve configuration, access and asset management firewall controls. The IRS recognizes the importance of maintaining solid firewall controls and has made considerable strides in deploying improvements that support these controls. We also appreciate recognition of the immediate response to correct issues such as password expiration dates, firewall asset inventory, and vulnerability scanning. We believe this response demonstrates the IRS's commitment to protecting our systems against cyberthreats and tax-related identity theft.

Attached is our detailed corrective action plan to address your recommendations. We strive to ensure that all of the facets of firewall management, hardware asset management, vulnerability management, network firewall configuration management, and dashboard analysis reporting provide the most effective protections to IRS systems. During the audit fieldwork, we took immediate action to address several items in the report. We believe this speaks to our commitment to ensuring continuous improvements in a timely manner.

The IRS values the continued support and assistance provided by your office. Should you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Frank Kist at (240) 613-4041.

Attachment



Attachment

Draft Audit Report – Firewall Administration Needs Improvement (Audit # 201920014)

RECOMMENDATION 1: The Chief Information Officer and the Chief, Criminal Investigation should conduct annual reviews of all firewall rulesets in accordance with agency policies and procedures.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. We will conduct annual reviews of all firewall rulesets in accordance with agency policies and procedures.

IMPLEMENTATION DATE: November 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services (UNS)

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.

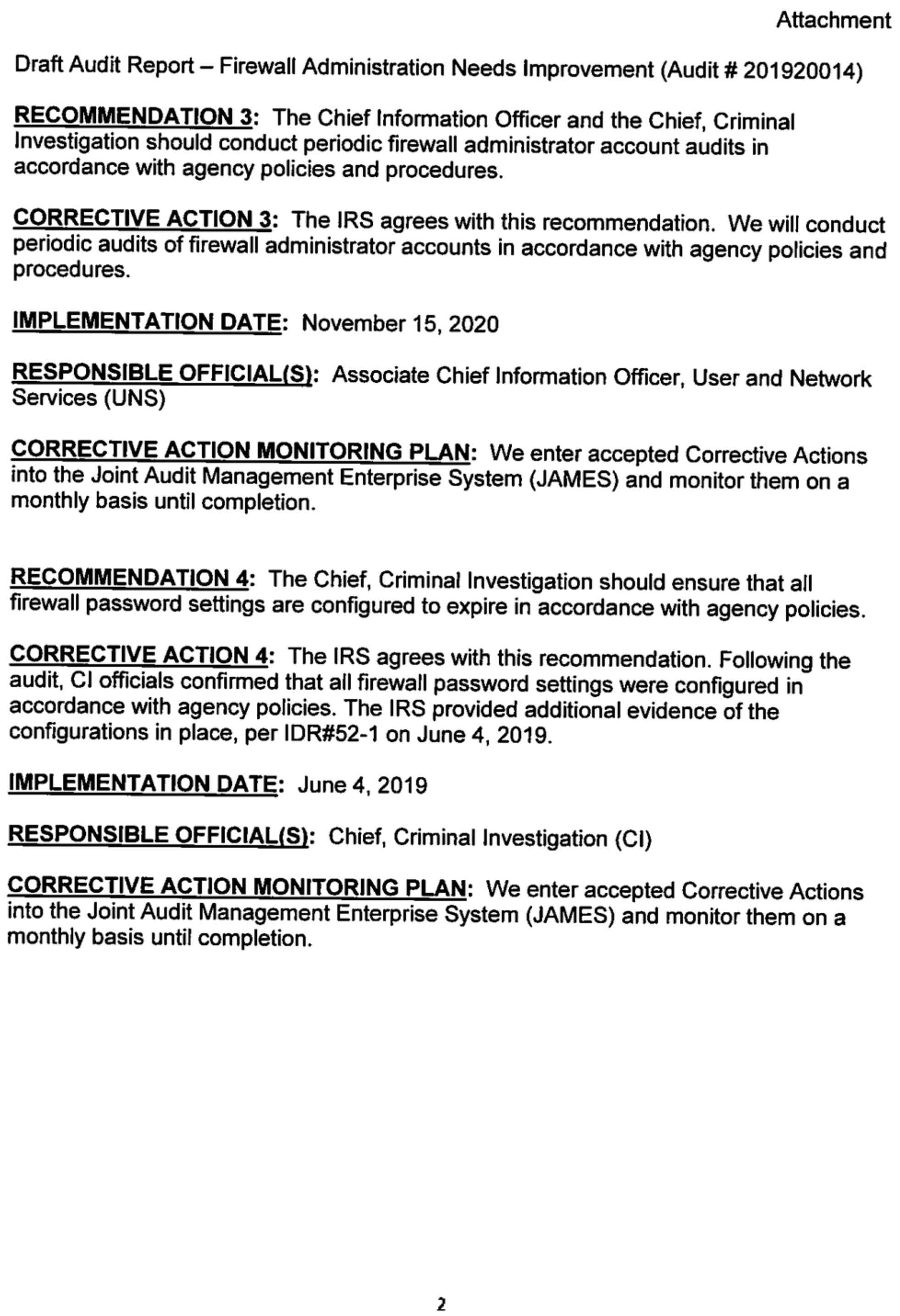
RECOMMENDATION 2: The Chief Information Officer and the Chief, Criminal Investigation should assign expiration dates not to exceed 365 days to firewall policies.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. We will assign designated expiration dates to firewall policies.

IMPLEMENTATION DATE: September 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services (UNS)

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.



Attachment

Draft Audit Report – Firewall Administration Needs Improvement (Audit # 201920014)

RECOMMENDATION 3: The Chief Information Officer and the Chief, Criminal Investigation should conduct periodic firewall administrator account audits in accordance with agency policies and procedures.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. We will conduct periodic audits of firewall administrator accounts in accordance with agency policies and procedures.

IMPLEMENTATION DATE: November 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services (UNS)

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.

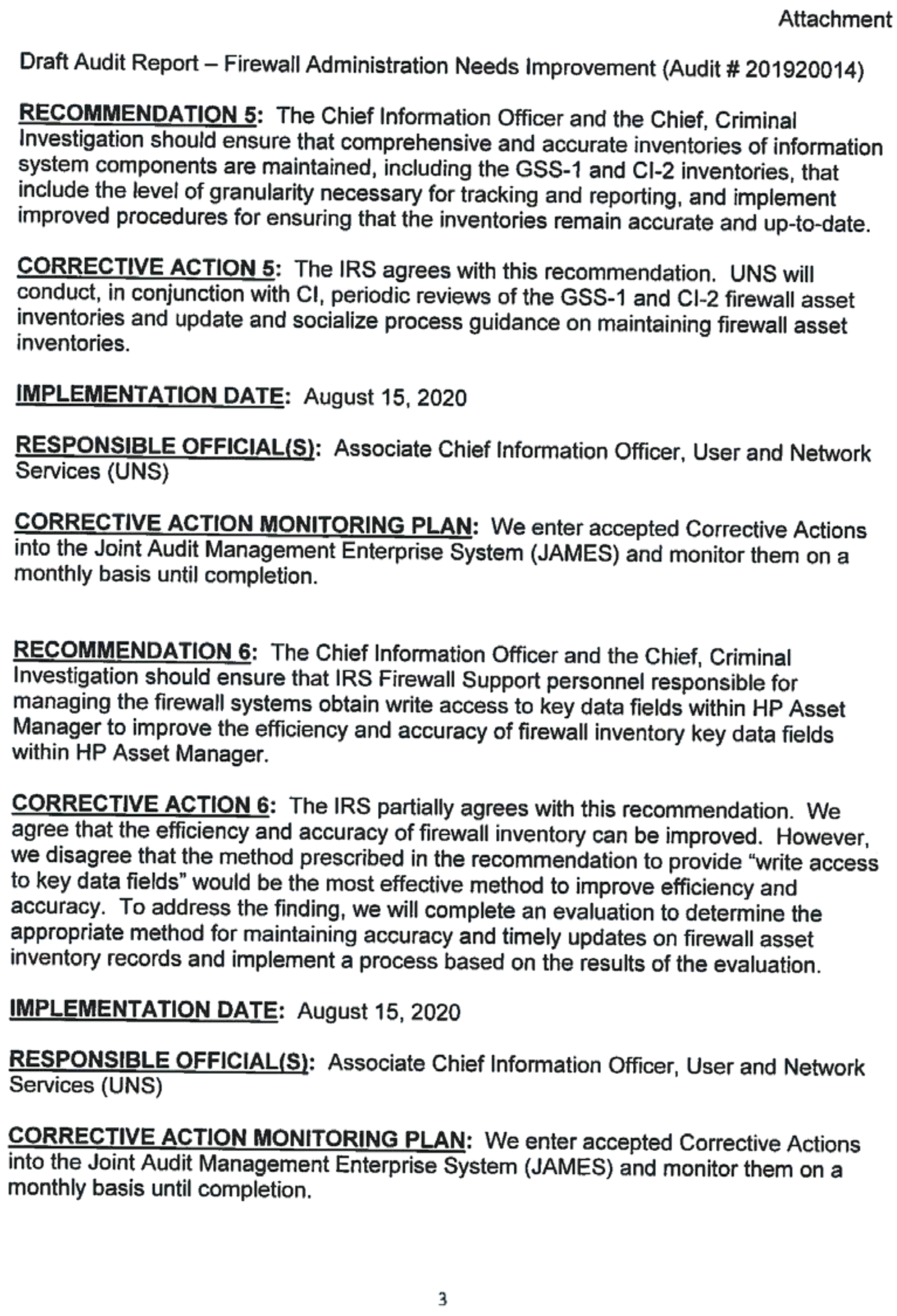
RECOMMENDATION 4: The Chief, Criminal Investigation should ensure that all firewall password settings are configured to expire in accordance with agency policies.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. Following the audit, CI officials confirmed that all firewall password settings were configured in accordance with agency policies. The IRS provided additional evidence of the configurations in place, per IDR#52-1 on June 4, 2019.

IMPLEMENTATION DATE: June 4, 2019

RESPONSIBLE OFFICIAL(S): Chief, Criminal Investigation (CI)

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.



Attachment

Draft Audit Report – Firewall Administration Needs Improvement (Audit # 201920014)

RECOMMENDATION 5: The Chief Information Officer and the Chief, Criminal Investigation should ensure that comprehensive and accurate inventories of information system components are maintained, including the GSS-1 and CI-2 inventories, that include the level of granularity necessary for tracking and reporting, and implement improved procedures for ensuring that the inventories remain accurate and up-to-date.

CORRECTIVE ACTION 5: The IRS agrees with this recommendation. UNS will conduct, in conjunction with CI, periodic reviews of the GSS-1 and CI-2 firewall asset inventories and update and socialize process guidance on maintaining firewall asset inventories.

IMPLEMENTATION DATE: August 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services (UNS)

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.

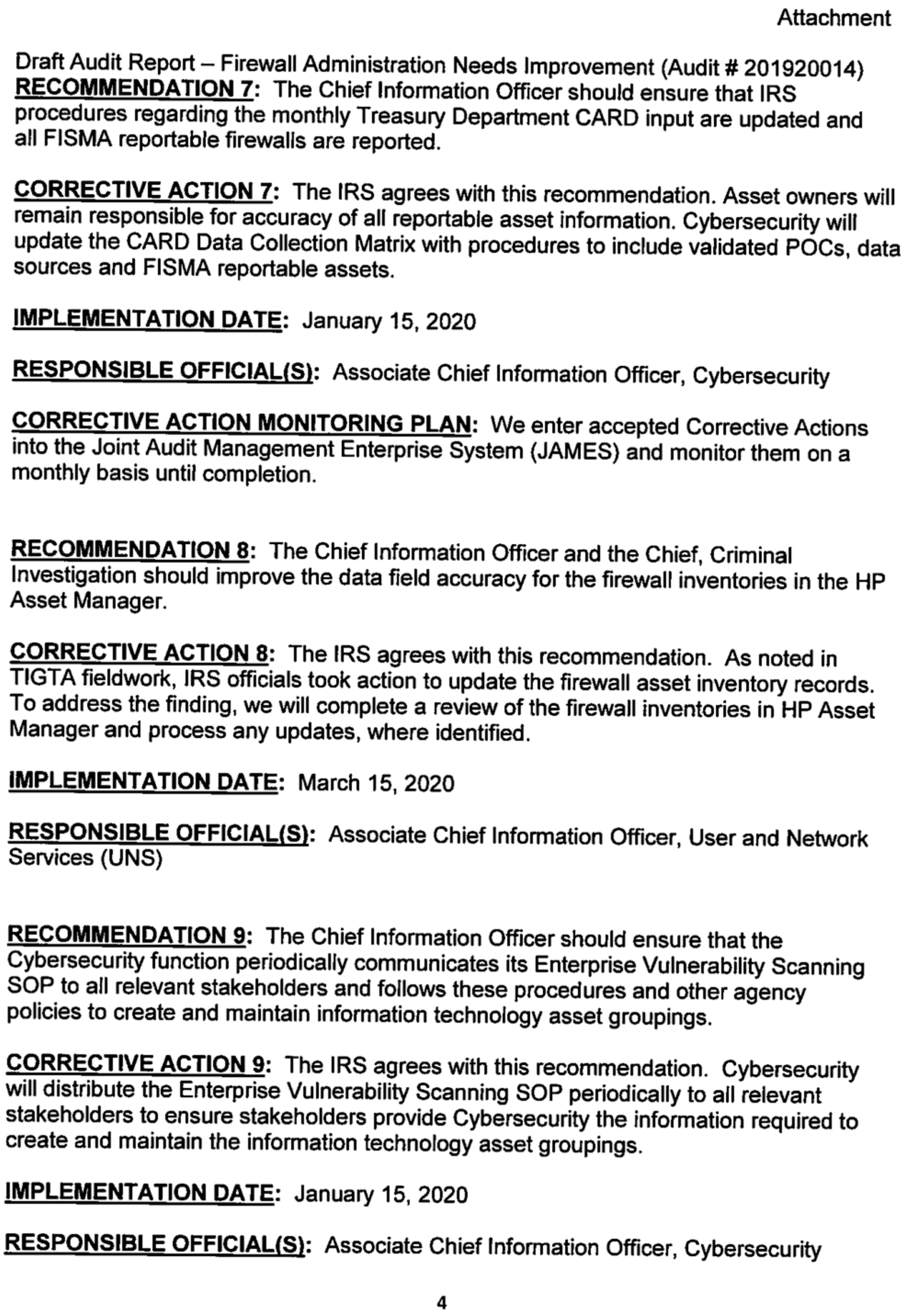
RECOMMENDATION 6: The Chief Information Officer and the Chief, Criminal Investigation should ensure that IRS Firewall Support personnel responsible for managing the firewall systems obtain write access to key data fields within HP Asset Manager to improve the efficiency and accuracy of firewall inventory key data fields within HP Asset Manager.

CORRECTIVE ACTION 6: The IRS partially agrees with this recommendation. We agree that the efficiency and accuracy of firewall inventory can be improved. However, we disagree that the method prescribed in the recommendation to provide "write access to key data fields" would be the most effective method to improve efficiency and accuracy. To address the finding, we will complete an evaluation to determine the appropriate method for maintaining accuracy and timely updates on firewall asset inventory records and implement a process based on the results of the evaluation.

IMPLEMENTATION DATE: August 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services (UNS)

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.



Attachment

Draft Audit Report – Firewall Administration Needs Improvement (Audit # 201920014)
RECOMMENDATION 7: The Chief Information Officer should ensure that IRS procedures regarding the monthly Treasury Department CARD input are updated and all FISMA reportable firewalls are reported.

CORRECTIVE ACTION 7: The IRS agrees with this recommendation. Asset owners will remain responsible for accuracy of all reportable asset information. Cybersecurity will update the CARD Data Collection Matrix with procedures to include validated POCs, data sources and FISMA reportable assets.

IMPLEMENTATION DATE: January 15, 2020

RESPONSIBLE OFFICIAL(S): 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 8: The Chief Information Officer and the Chief, Criminal Investigation should improve the data field accuracy for the firewall inventories in the HP Asset Manager.

CORRECTIVE ACTION 8: The IRS agrees with this recommendation. As noted in TIGTA fieldwork, IRS officials took action to update the firewall asset inventory records. To address the finding, we will complete a review of the firewall inventories in HP Asset Manager and process any updates, where identified.

IMPLEMENTATION DATE: March 15, 2020

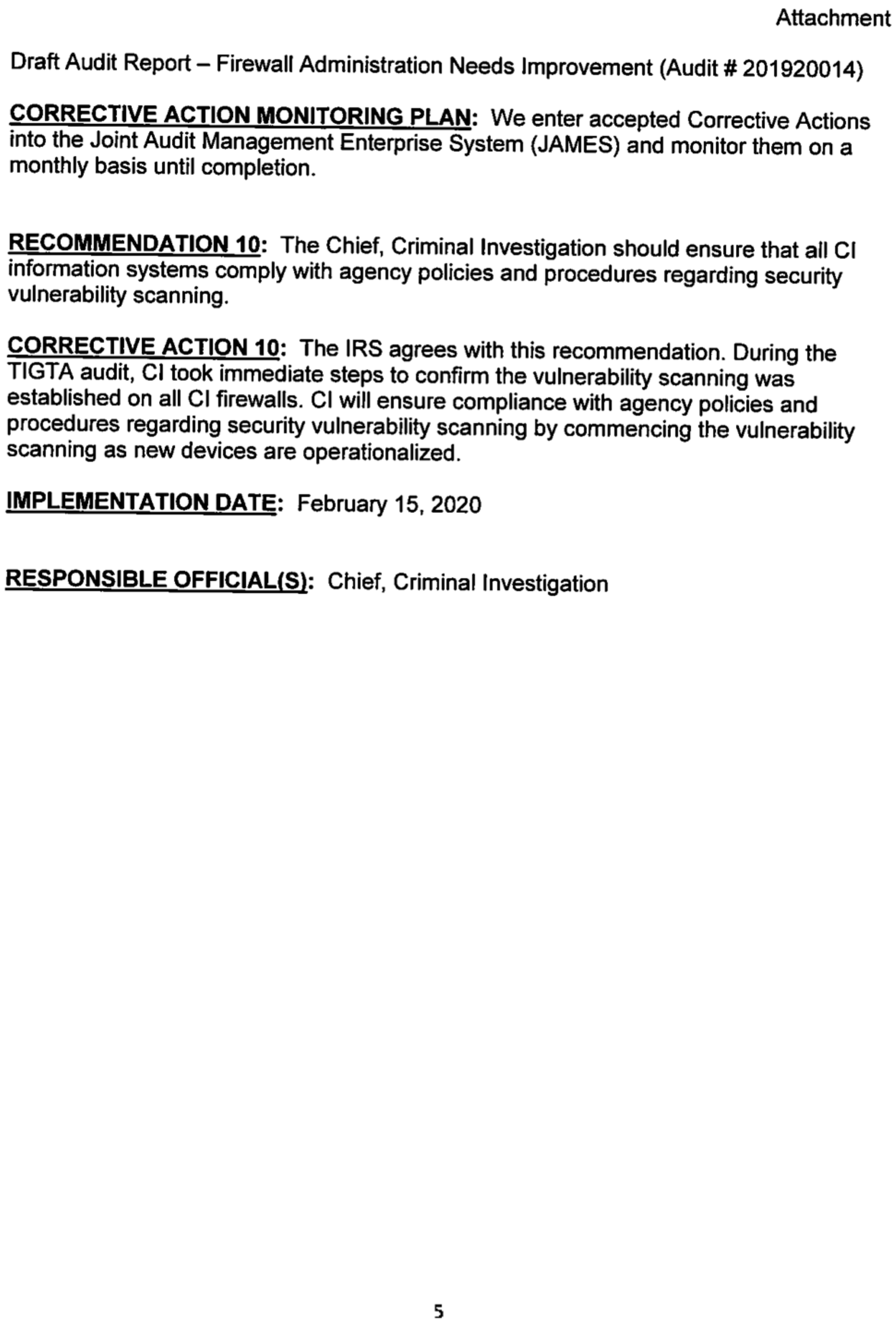
RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services (UNS)

RECOMMENDATION 9: The Chief Information Officer should ensure that the Cybersecurity function periodically communicates its Enterprise Vulnerability Scanning SOP to all relevant stakeholders and follows these procedures and other agency policies to create and maintain information technology asset groupings.

CORRECTIVE ACTION 9: The IRS agrees with this recommendation. Cybersecurity will distribute the Enterprise Vulnerability Scanning SOP periodically to all relevant stakeholders to ensure stakeholders provide Cybersecurity the information required to create and maintain the information technology asset groupings.

IMPLEMENTATION DATE: January 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity



Attachment

Draft Audit Report – Firewall Administration Needs Improvement (Audit # 201920014)

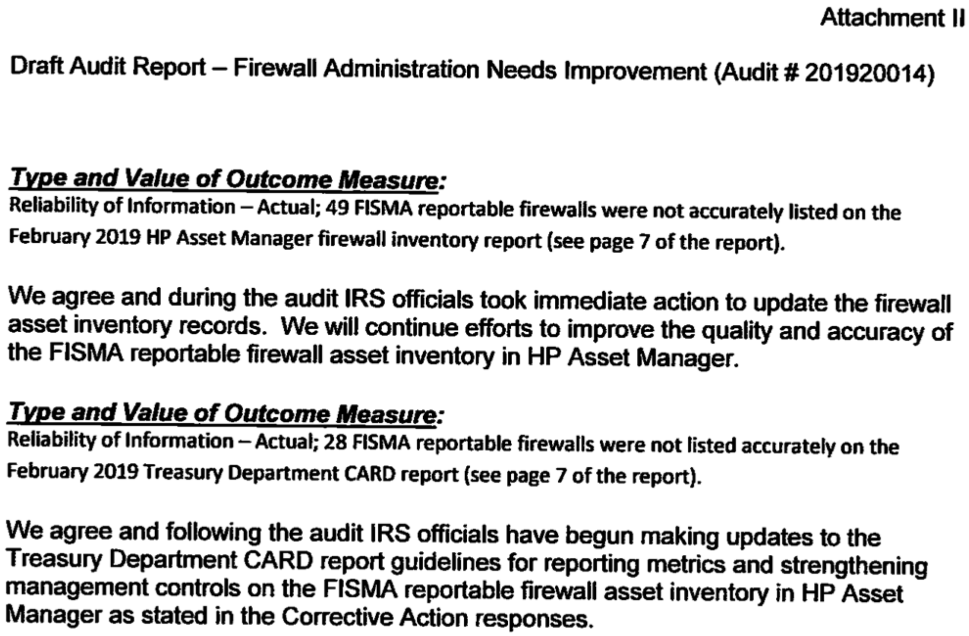
CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION 10: The Chief, Criminal Investigation should ensure that all CI information systems comply with agency policies and procedures regarding security vulnerability scanning.

CORRECTIVE ACTION 10: The IRS agrees with this recommendation. During the TIGTA audit, CI took immediate steps to confirm the vulnerability scanning was established on all CI firewalls. CI will ensure compliance with agency policies and procedures regarding security vulnerability scanning by commencing the vulnerability scanning as new devices are operationalized.

IMPLEMENTATION DATE: February 15, 2020

RESPONSIBLE OFFICIAL(S): Chief, Criminal Investigation



Attachment II

Draft Audit Report – Firewall Administration Needs Improvement (Audit # 201920014)

Type and Value of Outcome Measure:

Reliability of Information – Actual; 49 FISMA reportable firewalls were not accurately listed on the February 2019 HP Asset Manager firewall inventory report (see page 7 of the report).

We agree and during the audit IRS officials took immediate action to update the firewall asset inventory records. We will continue efforts to improve the quality and accuracy of the FISMA reportable firewall asset inventory in HP Asset Manager.

Type and Value of Outcome Measure:

Reliability of Information – Actual; 28 FISMA reportable firewalls were not listed accurately on the February 2019 Treasury Department CARD report (see page 7 of the report).

We agree and following the audit IRS officials have begun making updates to the Treasury Department CARD report guidelines for reporting metrics and strengthening management controls on the FISMA reportable firewall asset inventory in HP Asset Manager as stated in the Corrective Action responses.