TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating As Intended, but Improvements Are Needed

September 27, 2021

Report Number: 2021-20-065

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta

HIGHLIGHTS: The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating As Intended, but Improvements Are Needed

Final Audit Report issued on September 27, 2021 **Report Number 2021-20-065**

Why TIGTA Did This Audit

Endpoint devices (*e.g.,* laptops, desktops, and other applicable devices) are computer components that connect end users to an organization's networks and systems. These devices can also be a major source of vulnerabilities and a frequent target of attackers against networks. The IRS began deploying an Endpoint Detection and Response initiative before the President's Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021), that requires Executive Branch agencies to support proactive detection of cybersecurity incidents within the Federal Government infrastructure.

This audit was initiated to determine whether the Endpoint Detection and Response capability is effective to detect and provide information for the removal of any malicious activity deployed on or originating from endpoint devices.

Impact on Taxpayers

The IRS implemented the Endpoint Detection and Response solution to obtain a more complete picture of security incidents that occur on the IRS network by monitoring and obtaining detailed records of the incident from the affected workstation(s), which allows the IRS to conduct root cause analysis of identified threats. As a result, the security of taxpayer data on the IRS systems and network is improved.

What TIGTA Found

On May 7, 2020, the IRS began deploying the Endpoint Detection and Response solution, which analyzes various items, including the processes running on the workstations, memory artifacts, and other data points, and collects them on the computer. The collected data are correlated and compared to rules that have been established or associated with known indicators of compromise (*e.g.,* nation-state attackers and organized crime attacks). If anything is detected, the agent will generate an event/alert. From January 1, 2021, through April 30, 2021, Computer Security Incident Response Center analysts reviewed 735 alerts to determine whether these alerts should be elevated to an incident. TIGTA found that, to date, none of the alerts were elevated to an incident and that the Endpoint Detection and Response solution is effectively generating alerts from the workstations. The alerts are being tracked and worked.

While the IRS is effective with the alerts, the IRS can improve accounting for and fully deploying the Endpoint Detection and Response solution to all workstations enterprise-wide. In its *4th Quarter Fiscal Year 2020 Information Technology Investment Report*, the IRS reported that the Endpoint Detection and Response solution was at full operating capability. However, TIGTA found 91 confirmed workstations that were on the network and should have had the solution and 7,032 workstations that require further investigation to determine whether they are valid workstations and should have the solution installed. As a result, the Endpoint Detection and Response solution was not at full operating capability on all enterprise workstations.

Security management for operating the Endpoint Detection and Response solution could be strengthened. For example, Homeland Security Presidential Directive-12 credentials have not been implemented. In addition, system administrator accounts were not timely disabled for inactivity, *e.g.*, TIGTA found that two of the six system administrators had not accessed their accounts in the solution for more than 60 days yet the accounts were not disabled.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer ensure that all workstations in use are properly updated with the Endpoint Detection and Response solution, the Homeland Security credentials are used for access to the solution, and an effective process is developed to identify all users who are inactive beyond time requirements.

The IRS agreed with all of our recommendations. The IRS plans to review the workstations with an in use inventory status and properly deploy the Endpoint Detection and Response solution, and complete the implementation of credentials for access. In addition, the IRS stated that it has taken steps to address inactive user access.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 27, 2021

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating As Intended, but Improvements Are Needed (Audit # 202120006)

This report presents the results our review to determine whether the Internal Revenue Service's (IRS) Endpoint Detection and Response capability is effective to detect and provide information for the removal of any malicious activity deployed on or originating from endpoint devices. This review is part of our Fiscal Year 2021 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS Resources*.

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

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

Table of Contents

Appendices

Background

Endpoint devices (*e.g.,* laptops, desktops, and other applicable devices) are computer components that connect end users to an organization's networks and systems. These devices can also be a major source of vulnerabilities and a frequent target of attackers against networks. The cybersecurity community recognized the proliferation of endpoint devices, which widens an organization's attack surface for cyber bad actors to exploit. As a result, the industry is moving away from conventional host-based intrusion detection system functionality and more toward Endpoint Detection and Response (EDR)[1] product suites. The reasons that EDR solutions are important for businesses include the following considerations:

- The proactive approach – The reactive management approach of cyber threats and security issues for the network is no longer a prudent strategy. The current approach is to identify cyber threats and potential attacks before they occur and take remedial actions immediately. EDR solutions provide a proactive management approach of cybersecurity threats to a network.
- Better data monitoring and management – EDR solutions are designed in such a manner that they can collect and monitor data on each of the endpoints on a network and retain/archive the information in a database format, allowing for ease of access and management.
- Suitable for large-scale networks – Enterprises can have hundreds of thousands of endpoints on their networks. Such a large-scale network makes it more vulnerable to cyberattacks as it can be breached from multiple points. EDR solutions offer excellent scalability to accommodate a great number of devices.
- Powerful inbuilt data analytics – The analytical tools help identify cybersecurity threats to a network in the early phases of the threats' development and allow the enterprise to deal with them effectively.
- Compatibility and integration with other security tools – EDR solutions easily integrate with other security tools like malware analysis, network forensics, and threat intelligence to provide better overall security to a network.
- Observing endpoints without interfering – EDR solutions utilize the endpoints that are responsible for detection and response processes. Good EDR solutions use less space and have minimal footprints on the endpoints. As a result, they are lightweight and nonintrusive, and they facilitate continuous observing and monitoring of the endpoints without interfering with its functionalities.

The Information Technology organization's Cybersecurity function, along with support from its User and Network Services (UNS) function, are leading and managing the EDR solution. The Internal Revenue Service (IRS) purchased 11 EDR hardware appliances and 120,000 EDR security software agents plus maintenance and training for its enterprise at a cost of more than $4.6 million. On May 7, 2020, the IRS began deploying the EDR solution through the UNS Symantec Software Management Platform. This system relies on a workstation (*e.g.,* desktop,

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

laptops, and other devices, if applicable) to be connected to the IRS network in order for the software management platform and the agent to be properly installed to the workstation over the network.

According to the IRS, it implemented the EDR solution to obtain a more complete picture of security incidents that occur on the IRS network by monitoring and obtaining detailed records of an incident from the affected workstation(s), which allows the IRS to conduct root cause analysis of identified threats. In addition, the Cybersecurity function determined that EDR solutions provide better detection and mitigation around advanced persistent threats through the analysis of indicators of compromise from nation-state attackers and organized crime attacks in real time. The EDR solution also provides the ability to replay and analyze inbound and outbound network traffic across the IRS enterprise network. This is significant because the IRS network includes systems with taxpayer data.

Specifically, to provide a complete picture of security incidents occurring on the network using detailed records from the workstations, the EDR agent continuously monitors key items on the endpoints (*i.e.*, workstations).[2] The EDR solution looks at various items, including the processes running on the workstations, memory artifacts, and other data points, and collects them in an on-site (on the computer) cache. The agent automatically collects and retains data from the workstation from 10 minutes prior to a trigger for the security event and up to 10 minutes past the event to provide a complete timeline of the event. The cached data are correlated and compared to rules within the EDR solution that have been established/associated with known indicators of compromise (*e.g.,* nation-state attackers and organized crime attacks). This comparison is performed in real time. If anything is detected, the agent will generate an event/alert, which is also sent to the management environment. This provides the data necessary to see what was occurring on the workstation and gives insight into the potential threat. The agent also sends e-mail messages of the event information to the Computer Security Incident Response Center's (CSIRC) mailbox that is monitored 24 hours, 7 days a week. CSIRC analysts use the information to determine whether any mitigating actions need to be taken. They can then quantify the attack vector and determine how to proceed. In addition, the EDR solution is tied into the CSIRC Splunk environment.

To reaffirm the importance of this technology, the President signed Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021), that requires Federal Civilian Executive Branch agencies to deploy an EDR initiative to support proactive detection of cybersecurity incidents within the Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response.

Results of Review

When the IRS initially deployed its EDR solution in May 2020, [redacted]. In the long term, the IRS [redacted].

[2] Initially, the IRS planned to deploy the agent to workstations and servers; however, filing season moratoriums and server ownership impacted its deployment, and the servers are planned for a phase 2 deployment.

While typical EDR solutions can be designed to also remove/mitigate detected threats, the IRS uses other mitigating controls but remains open to the solution's capabilities.

We reviewed the alert logs generated by the EDR solution and found that alerts are delivered through e-mail messages to the appropriate personnel and are forwarded to the [redacted]. Currently, CSIRC analysts log all alerts issued from the EDR solution. However, prior to December 1, 2020, they did not have documentation to support logging actions. From January 1, 2021, through April 30, 2021, there were 735 alerts generated by the EDR solution, and there were 735 line items in the CSIRC tracking log. CSIRC analysts review the alerts to determine whether the alert should be elevated to an incident and mitigating actions taken. Figure 1 lists the 735 alerts as categorized by the analysts.

Figure 1: List of the 735 Alerts from the EDR Solution by Category

Category Name	Number of Alerts	Description
False Positive	724	An alert that incorrectly indicates that a vulnerability is present. Examples included possible Ransomware and Bloodhound Scanner (Penetration Testing and Code Analysis).
Valid Risk Blocked	7	An alert that identified a legitimate potential risk, but the risk was blocked by the appropriate defense mechanism. An example included a renamed copy of a Windows utility that could be used legitimately or by attackers.
Investigation Created	2	CSIRC analyst determined that the alert warranted further review. The review included a search of a cyber threat management application and other CSIRC intelligence records as something that was already known. Examples included suspicious files in an Outlook attachment and a credential stealer.
Previously Blocked	1	This event previously occurred and was already blocked as appropriate. A prior occurrence with a record in a cyber threat management application. After a lengthy review, the analyst determined that it was a valid process associated with resetting a user's password.
Inconclusive	1	The reviewer could not categorize this alert definitively in another category and searched another forensic tool. The alert was for suspicious files in an Outlook attachment that was subsequently closed.
Total	**735**	

Source: CSIRC analysts' review of alerts generated from the IRS's EDR solution from January 1, 2021, through April 30, 2021.

We found that none of the alerts were elevated to an incident and that the EDR solution is effectively generating alerts from the workstations with the EDR solution. The alerts are being properly tracked and worked. The alerts were caused by either internal testing, legitimate processes, or indicators of the appearance of a possible threat (*e.g.,* threat emulation exercises, Powershell®, Bloodhound, and potential credential theft attempts), which the EDR solution incorporates rules to identify as potential for concern. After CSIRC analysts conducted their reviews, they decided that none of the alerts qualified to be an incident.

While the IRS is effective in generating and tracking alerts from the EDR solution on workstations, the IRS can improve:

- Accounting for and fully deploying the EDR solution to all workstations enterprise-wide.
- Security management for operating the EDR solution.

The IRS began deploying an EDR initiative before the President's Executive Order 14028 required Executive Branch agencies to deploy such an initiative; however, addressing our findings will assist the IRS with supporting the proactive detection of cybersecurity incidents within the Federal Government infrastructure.

The Endpoint Detection and Response Solution Was Neither Fully Accounted for nor Deployed to All Required Workstations Enterprise-Wide

The IRS began with an incremental deployment plan when it started to deploy the EDR solution to approximately 1,800 workstations on May 7, 2020. Within five days, it had deployed the EDR solution to more than 30,000 workstations. By September 21, 2020, the UNS function determined that 88,595 workstations were eligible to receive the EDR solution and reported a successful deployment of the EDR solution to 86,593 (97.74 percent) of eligible workstations. Cybersecurity personnel confirmed that the number coincided with the number of workstations recorded within the EDR management environment. In its *4th Quarter Fiscal Year 2020 Information Technology Investment Report*, the IRS reported that the EDR was at full operating capability.

The IRS reported that the EDR was at full operating capability. However, as a result of our discussions with the IRS and further analyses, we concluded that the EDR solution was not at full operating capability on all enterprise workstations.

We requested that the UNS function provide a list of the workstations in use enterprise-wide from May 7, 2020, through December 31, 2020,[3] and that the Cybersecurity function provide a list of all workstations with the deployed EDR solution from the same time period. The UNS function provided the January 31, 2021, status of workstations that were in use as of December 31, 2020, which totaled 111,283 workstations. However, UNS personnel explained that "in use" was historically set as a financial qualification to indicate an asset was being used in some capacity by the IRS organization and not as an indication of it being on the network. In addition, UNS personnel stated that their list could include duplicates as some assets were taken in and out of use multiple times during the time period we requested.

The Cybersecurity function's list totaled 96,441 workstations with the deployed EDR solution. When we compared the host name of the workstations from both lists, we identified 25,245 workstations that were on the UNS list but not on the Cybersecurity list. Further review of the data allowed us to remove 16,288 workstations from the list, which comprised of 14,931 workstations that were in stock, 1,329 workstations that were missing, and 28 workstations that were retired. We also removed 1,631 workstations that were duplicates

[3] The UNS list of workstations is from the Asset Manager module in the Knowledge Incident/Problem Service Asset Management System.

and those that either received the defense in-depth capability[4] and/or the EDR solution after our cutoff date, which left a difference of 7,326 workstations that potentially did not have the EDR solution. In April 2021, we provided a list of the 7,326 workstations to the IRS for review.

- For the 7,326 workstations, the IRS stated that 10 were not eligible for the EDR solution.
- For the remaining 7,316 workstations:
    - As of May 17, 2021, a Cybersecurity official conducted an analysis to determine how many of the 7,316 workstations had the EDR solution and was able to provide the following information on 317 workstations:
        - 61 workstations had the EDR solution even though they did not have the IRS's in-depth defense capability that Cybersecurity used to determine whether the workstation needed the EDR solution.
        - 256 workstations had the defense in-depth capability, of which:
            - 203 had the EDR solution.
            - 53 were confirmed as not having the EDR solution.
    - For the remaining 6,999 workstations, which had neither the defense in-depth capability nor the EDR solution, Enterprise Services personnel were unable to provide specific reasons why the EDR solution was not installed during our audit work and stated it could take a month or more to research because it is a manual process. However, UNS personnel provided the following possible explanations for the workstations that were in use but did not have the EDR solution.
        - The asset is actually in use and is not required to be on the network (*e.g.,* Integrated Submission and Remittance Processing or Service Center Recognition Image Processing System workstations/servers or test equipment for projects that are not on the network).
        - The asset was in use, but an inventory transaction occurred that took the asset off the network without the inventory transactional update being reported via the install, move, add, or change options for updates to the IRS's asset manager.
        - The asset was in use, but an inventory transaction occurred that took it off the network and an install, move, add, or change option was submitted, but there may be a timing discrepancy between the time the option was processed and when the asset showed up on the report.
        - The asset in use may have a bad security software agent; therefore, it does not show up on the network.
        - Due to the Coronavirus Disease 2019 pandemic, the IRS fast tracked the assignment of individual laptops to users who previously shared desktops so that they could telework. The priority was to get the laptops out to the users. As a result, there are ongoing follow-up efforts to turn in and update the workstation assignments in the asset manager.

[4] A Cybersecurity official used the workstations that appear online by checking in through the defense in-depth capability to determine whether the workstations did or did not have the EDR solution.

In addition, we identified, in a separate analysis with a Cybersecurity official's assistance, 144 workstations that were shown as connected to the network as of April 9, 2021, without the EDR solution. We also provided these results to the IRS in April 2021 for review. For these 144 workstations:

- 5 were not currently eligible for the EDR solution because they were Apple™ devices.
- 3 were blacklisted, as they were not approved to be on the network.
- 33 were found (on April 27, 2021) to be in stock but not in use.
- 38 appeared on the IRS's network between May 21, 2021, and June 2, 2021, and it was confirmed that they did not have the EDR solution deployed.
- 32 either had both the EDR solution and the defense in-depth capability or only the EDR solution.
- 33 were not identified on the network when a Cybersecurity function official conducted a subsequent analysis, and as such, the current inventory status of those devices is unknown.

In total, we are concerned with the 91 confirmed workstations[5] without the EDR solution and 7,032 workstations[6] without a known explanation for why the EDR solution is not deployed to them. These workstations will require further investigation to determine whether they are valid workstations and should have the solution installed. The unreliability of the status of the workstations impacts the Cybersecurity function's proactive approach of identifying cyber threats and potential attacks before they occur so they can be remediated immediately. As a result of our discussions with the IRS and further analyses, we concluded that the EDR solution was not at full operating capability on all eligible enterprise workstations.

The UNS function has responsibility to ensure that all enterprise security software, including the EDR solution, is installed and working properly per tested and agreed-upon configurations. Formalized coordination occurs during the initial testing and installation phase and during subsequent upgrades that are needed to ensure that the latest versions of the software are installed. Further, for the life of the product, the UNS function is responsible for ensuring that the software is installed, with the Cybersecurity function providing context to the UNS function on any communication issues noticed via tickets from the asset manager, e-mail, Skype, and verbal methods. At present, the Cybersecurity function relies on the UNS function, as the administrators of the workstation platforms, to ensure that the product is installed on any applicable machine that will be brought online and used for IRS business. The Cybersecurity function is making attempts to verify that the installation of the EDR solution is working correctly on each system, although Cybersecurity personnel admitted that challenges exist on how to best obtain missing/misconfigured installations and how to best rectify it as quickly as possible.

The UNS function could have taken a more proactive approach to ensure that all deployed assets had the EDR solution or to incorporate a means to continuously verify that the agent is running correctly. By not ensuring that all eligible workstations have the EDR solution installed,

[5] Adding the 38 confirmed workstations in the previous bullet with the aforementioned 53 confirmed workstations from the previous page yields 91 confirmed workstations without the EDR solution.

[6] The 7,032 workstations are composed of the 6,999+33 workstations from the bullets above.

the IRS will be unable to monitor and obtain detailed records of incidents on all workstations and conduct root cause analyses of identified threats. These gaps of EDR deployments may also give a false sense of security and possibly lead to missed opportunities to quickly mitigate incoming cyberattacks at the workstation.

The Chief Information Officer should:

Recommendation 1: Ensure that UNS personnel promptly review the workstations in the in use inventory status and on the network to ensure that the EDR solution is properly deployed to all workstations.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, UNS, will review workstations in an in use inventory status that are on the network and ensure that the EDR solution is properly deployed.
>
> > **Office of Audit Comment:** The June 15, 2022, corrective action implementation date does not constitute a prompt review to ensure that the EDR solution is properly deployed to all workstations. The time gap may possibly lead to missed opportunities to quickly identify and mitigate incoming cyberattacks at the workstation and give a false sense of security.

Recommendation 2: Ensure that the EDR solution is deployed on all workstations that will be brought online and used for IRS business prior to being issued to users.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, UNS, will integrate the EDR solution into the workstation build process so that the solution is installed on newly built workstations as well as workstations being re-imaged.

Recommendation 3: Ensure that UNS personnel inform the Cybersecurity function of systems no longer on the network (*e.g.,* retired, stolen, or excessed) so it can update its EDR inventory list when assets are no longer viable within the enterprise.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, UNS, will set up automated communications to inform the Cybersecurity function when assets have a final disposition.

Security Management for Operating the Endpoint Detection and Response Solution Could Be Strengthened

The *Standards for Internal Control in the Federal Government*[7] state that management designs control activities for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system. Objectives for security management include confidentiality, integrity, and availability. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Integrity means that information is safeguarded against improper modification or destruction, which

[7] Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government*, pp 54 and 55 (Sept. 2014).

includes ensuring the information's nonrepudiation and authenticity. Availability means that data, reports, and other relevant information are readily available to users when needed.

Homeland Security Presidential Directive-12 (HSPD-12) credentials have not been implemented for access to the EDR solution

The HSPD-12 is designed to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. [redacted].

During our audit work, we found that the Public Key Infrastructure–based authentication via the HSPD-12 credential had not been implemented for the EDR solution in accordance with IRM guidance. According to a Cybersecurity function official, initial efforts to ensure proper implementation of the required HSPD-12 directive were not successful due to an issue the Cybersecurity function's EDR team reported to the vendor at the time of testing. A new release of the EDR solution has just been implemented, in which efforts toward meeting the directive are being reviewed. [redacted], which will also meet the requirements of the directive and will hopefully allow for more configuration granularity than what has been previously tested. The official continued that they are working toward a solution that they believe should be in place well before the end of Fiscal Year 2021. Until the IRS deploys HSPD-12 card access to the EDR solution, it cannot take advantage of two-factor authentication and enhanced protection for accessing the EDR solution.

EDR system administrator accounts were not timely disabled due to inactivity

Administrator accounts (also known as privilege accounts) provide users with the authorization to override, or bypass, certain security restraints and may include permissions to perform such actions as shutting down systems. Because these accounts basically allow a user to do anything on the system, [redacted].

Figure 2: *********3****************

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted].

In March 2021, we found that [redacted]. Internal guidelines state that employees who perform system administrator tasks shall have two user accounts – one for administrator duties and one for general user activity (*i.e.,* role-based access). The system administrators' leveraging of the application program interface for service calls appeared to be for general user activity.

Currently, the IRS is using Active Directory domain accounts to identify all EDR solution users, including administrators. According to a Cybersecurity official, the IRS does not have an effective process to identify active and inactive users through the EDR solution as they are not using the local accounts in the EDR solution. As a result, if the user is approved and then removed, the account is removed from the groups in Active Directory, which removes all access. There is not an automated mechanism within the EDR solution to remove a user due to inactivity from the Active Directory domain group. This issue would require further investigation and is something that would possibly require manual intervention to implement. Until the IRS establishes an effective process, we believe that poorly managed system administrator privileged accounts leave organizations exposed to security breaches such as accidental harm and malicious activity.

Not all EDR solution users were added to their assigned Active Directory domain groups

[redacted]. There are four roles in each of the three Active Directory domain groups in the EDR management environment – production, test, and development. The four roles are administrator, analyst, senior analyst, and investigator.

The separation of duties policy is broad and includes guidance regarding role assignments, which is what we used to review all 42 EDR solution users to evaluate whether they were properly assigned to their correct domain group. We found four (10 percent) users who were not added to all of their assigned Active Directory domain groups but were located in only their system administrator or investigator domain groups. Specifically, we found the following issues:

- One user was not found as an investigator in the production domain group. In the Online 5081 system, the user was approved as an investigator in the production domain group. However, we did not find the user in the Active Directory production domain group. A Cybersecurity official stated that this user is a member in an analyst role in the production domain group, which has fewer rights than the investigator role.
- One user was not found as an investigator in the production, test, and development domain groups. In the Online 5081 system, the user was approved as an investigator for all three groups. However, in Active Directory, the user was not included in any of the three domain groups. A Cybersecurity official stated that this was a management oversight, as this user should be a member of these groups.
- One user was not found as a senior analyst in the development domain group. In the Online 5081 system, the user was approved as a senior analyst in the stated domain group; however, the user was not included in Active Directory as a senior analyst in the development domain group. A Cybersecurity official stated that the analyst role has fewer capabilities, but this is where the majority of the analysts are assigned. This user was added to this lesser role to have similar functionality with other analysts for troubleshooting purposes. They did not update the Online 5081 system because the role has fewer rights and is used for testing.
- One user was not placed as a senior analyst in the test domain group. In the Online 5081 system, the user was approved as a senior analyst in the test domain group; however, in the Active Directory group, the user was not approved. A Cybersecurity official stated this was a management oversight, as this user should be a member of this group.

The IRS plans to make changes to two of the four Active Directory domain groups – the user who was not found as an investigator in the production, test, and development domain groups and the user who was not placed as a senior analyst in the test domain group. However, a Cybersecurity official believes there is minimal risk for the remaining two users' Active Directory domain group placements. For further clarity, the Cybersecurity official offered that the noted users being members of "system administrator domain groups," the only domain groups designated to function as "system administrators," are those tied specifically to the "administrator" role in each of the three EDR management environments.

For proper reporting and auditing moving forward, the IRS stated that the Cybersecurity function's EDR team will work to ensure that the Online 5081 system (soon to be replaced with the Business Entitlement Access Request System) user assignments map correctly to the associated Active Directory groups for access to the environment for proper continuity. Until the role mapping is corrected, we caution that, if the IRS does not properly manage its role assignments, it will be unable to monitor the system administrator users' activity beyond the administrator and investigator roles in the EDR management environment. Accuracy in role assignment management provide for an independent check on the accounting for work performed and reduces the risk of inappropriate employee actions.

No documented evidence that EDR system default passwords were timely changed

[redacted].

Factory default software configuration for embedded systems, devices, and appliances often include simple, publicly documented passwords. Default passwords for EDR solution appliances may not have been changed before or immediately after the solution was placed into production beginning May 7, 2020. During our review, we found the passwords for nine system administrator local accounts were last changed on December 1, 2020. Further interviews with a Cybersecurity official revealed that the nine local system accounts in question did not have their default password reset by the Cybersecurity EDR team after the installation of the appliances; however, they were disabled from being logged into as suggested by the vendor back in June 2019 during the initial configuration set-up and when they had not yet started pulling the event logs into [redacted]. However, the official was unable to get the exact date and did not have documentation to when the passwords were disabled. Allowing default passwords and not disabling access to accounts unnecessarily exposes the EDR solution to unauthorized access, which may result in damage or data loss.

The Chief Information Officer should:

Recommendation 4: Ensure that HSPD-12 credentials are used for access to the EDR solution, as required for access to all systems.

> **Management's Response:** The IRS agreed with this recommendation. The IRS stated that the integration of HSPD-12 credentials has been implemented on all test, development, and passive production appliances. All active production appliances will have the recommended corrective action implemented per the noted implementation date.

Recommendation 5: Develop an effective process to identify all EDR solution users who are inactive beyond time requirements.

> **Management's Response:** The IRS agreed with this recommendation. The IRS stated that it has taken steps to address a manual method to extract and qualify inactive access.

Recommendation 6: Ensure that the Cybersecurity EDR team correctly maps user assignments to the associated Active Directory domain group(s) via the access control system.

> **Management's Response:** The IRS agreed with this recommendation. The IRS stated that it has taken steps to correctly map user assignments to the associated Active Directory domain groups via the access control system.

Recommendation 7: Maintain documentation to support that default password changes or disabling occurred before or immediately after an application has been implemented.

> **Management's Response:** The IRS agreed with this recommendation. The IRS stated that it has taken steps to document the default password changes before or immediately after an application has been implemented.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the EDR capability is effective to detect and provide information for the removal of any malicious activity deployed on or originating from endpoint devices. To accomplish our objective, we:

- Obtained a list of all workstations with the deployed EDR solution from the Cybersecurity function and a list of workstations in use from the UNS function. We compared the two lists to determine whether any workstations in use did not have the deployed EDR solution. We reviewed the exceptions to determine whether they were devices that the IRS decided not to deploy the EDR solution.

  Discussed the exceptions with the IRS to determine the cause and the planned actions to ensure that the EDR solution is successfully deployed to all workstations. In addition, we determined whether the IRS followed its policies and procedures for deploying the EDR solution.
- Obtained and reviewed the IRS's policies and procedures related to the EDR solution capabilities and intrusion detection and response to determine whether they were in accordance with applicable Federal policies and guidelines.
- Reviewed the EDR solution's appliance passwords to verify whether the IRS changed the EDR solution default passwords for access (*i.e.,* system administrators) within the software.
- Obtained a list of all staff with access to the EDR solution and the roles assigned to each person, and compared the assigned roles for the staff members to their assigned duties to ensure that they were appropriate. In addition, we determined whether there was an appropriate level of separation of duties regarding role assignments among the different roles and staff members.
- Obtained the alerts generated from the EDR solution for the period May 1, 2020, through April 30, 2021. We obtained the reviewers' alert tracking logs for the period December 1, 2020, through April 30, 2021. We compared the alerts and logs to determine whether they were accurately captured and whether they resulted in incidents.

Performance of This Review

This review was performed with information obtained from the Cybersecurity and UNS functions in Augusta, Georgia, at the New Carrollton Federal Building in Lanham, Maryland, and at the Enterprise Computing Center–Memphis in Memphis, Tennessee, during the period October 2020 through July 2021. 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Kent Sagara, Director; Deborah Smallwood, Audit Manager; Suzanne Westcott, Lead Auditor; and Michael Segall, Senior Auditor.

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of the data from the UNS function's inventory of in use workstations. We requested the in use date and any assets that were changed to in use status for the period of May 7, 2020, through December 31, 2020. We confirmed the in use date in the data as May 7, 2020, and the dates the assets were changed to in use status were from May 8, 2020, through December 31, 2020. We requested that the UNS function include the media access control address, a unique address for the workstation; the operating system; and the host name in the data. We observed and UNS function personnel stated that some of the workstations did not include the requested information. For the Cybersecurity function's inventory of workstations with the deployed EDR solution, we requested the installation date and the media access control address and observed that some of the workstations did not include the requested information. We determined that the data were sufficiently reliable for the purposes of this report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the IRS information technology security, policy, and guidance that addressed business role account inactivity, separation of duties, application role account, authentication management control, and the system security plan. We evaluated these controls by interviewing IRS personnel responsible for the deployment and operation of the EDR solution for security purposes, reviewing data files, and reviewing relevant documentation.

Appendix II

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 – Potential; 7,032 (6,999+33) unaccounted-for workstations in use and included workstations that were on the network, but all were without the EDR solution (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

The Cybersecurity function provided a list of workstations in use with the deployed EDR solution from May 7, 2020, to December 31, 2020, and the UNS function provided a list of workstations in use as of December 31, 2020. When we compared the host name of the workstations from both lists, we identified 25,245 workstations on the UNS function list that were not on the Cybersecurity function list. Further review of the data allowed us to remove:

- 14,931 workstations that were in stock.
- 1,329 workstations that were missing.
- 28 workstations that were retired.
- 1,631 duplicate workstations and those that either received the defense in-depth capability and/or EDR solution after our cutoff date.
- 10 workstations were not eligible for the EDR solution.
- 317 workstations for which a Cybersecurity function official provided us with an updated status of the EDR solution deployment as of May 17, 2021.

This resulted in 6,999 in use workstations without the EDR solutions installed.

In our separate analysis of 144 workstations that were showing as connected to the network without the EDR solution, a Cybersecurity function official conducted a subsequent analysis and confirmed that the inventory status was unknown for 33 of the 144 workstations based on available data.

Type and Value of Outcome Measure:

- Protection of Resources – Potential; 91 (53+38) workstations that did not have the deployed EDR solution (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

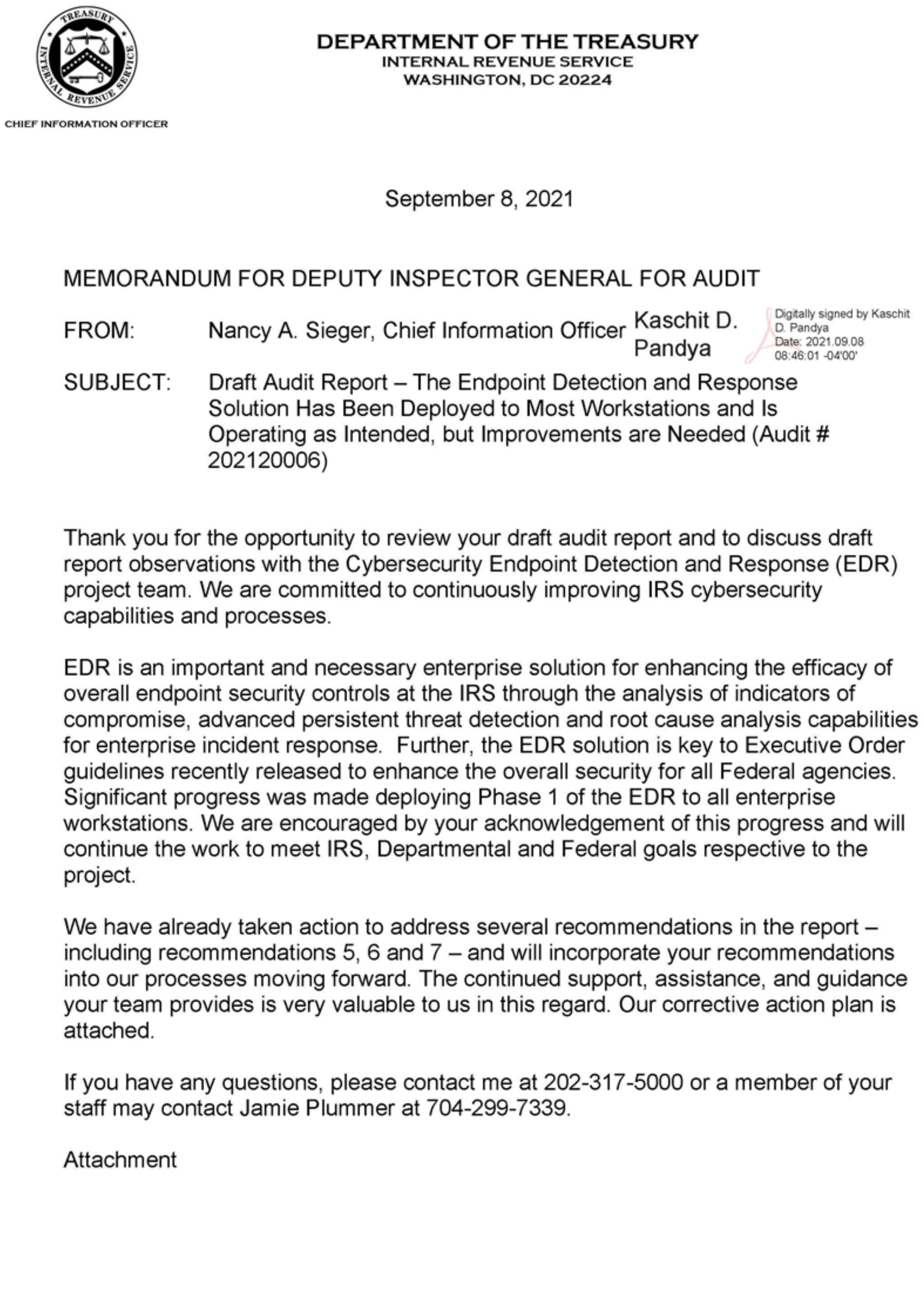
As of May 17, 2021, a Cybersecurity function official conducted an analysis of the workstations that we determined were in use but did not have the deployed EDR solution. The official found

256 workstations that had the defense in-depth capability, of which 203 had the EDR solution. The remaining 53 workstations did not have the deployed EDR solution.

We also identified, in a separate analysis with a Cybersecurity function official's assistance, 38 additional workstations connected to the network between May 21, 2021, and June 2, 2021, that did not have the deployed EDR solution.

Appendix III

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 8, 2021

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger, Chief Information Officer Kaschit D. Pandya

Digitally signed by Kaschit D. Pandya
Date: 2021.09.08 08:46:01 -04'00'

SUBJECT: Draft Audit Report – The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating as Intended, but Improvements are Needed (Audit # 202120006)

Thank you for the opportunity to review your draft audit report and to discuss draft report observations with the Cybersecurity Endpoint Detection and Response (EDR) project team. We are committed to continuously improving IRS cybersecurity capabilities and processes.

EDR is an important and necessary enterprise solution for enhancing the efficacy of overall endpoint security controls at the IRS through the analysis of indicators of compromise, advanced persistent threat detection and root cause analysis capabilities for enterprise incident response. Further, the EDR solution is key to Executive Order guidelines recently released to enhance the overall security for all Federal agencies. Significant progress was made deploying Phase 1 of the EDR to all enterprise workstations. We are encouraged by your acknowledgement of this progress and will continue the work to meet IRS, Departmental and Federal goals respective to the project.

We have already taken action to address several recommendations in the report – including recommendations 5, 6 and 7 – and will incorporate your recommendations into our processes moving forward. The continued support, assistance, and guidance your team provides is very valuable to us in this regard. Our corrective action plan is attached.

If you have any questions, please contact me at 202-317-5000 or a member of your staff may contact Jamie Plummer at 704-299-7339.

Attachment

1

Draft Audit Report – The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating as Intended, but Improvements Are Needed (Audit #202120006)

RECOMMENDATION 1
The Chief Information Officer should ensure that UNS personnel promptly review the workstations in the in-use inventory status and on the network to ensure that the EDR solution is properly deployed to all workstations.

CORRECTIVE ACTION #1
The IRS agrees with this recommendation. We will review workstations in an in use inventory status that are on the network and ensure that the EDR solution is properly deployed.

IMPLEMENTATION DATE
June 15, 2022

RESPONSIBLE OFFICIALS
Associate Chief Information Officer, User Network & Services

CORRECTIVE ACTION MONITORING PLAN
We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress monthly until completion.

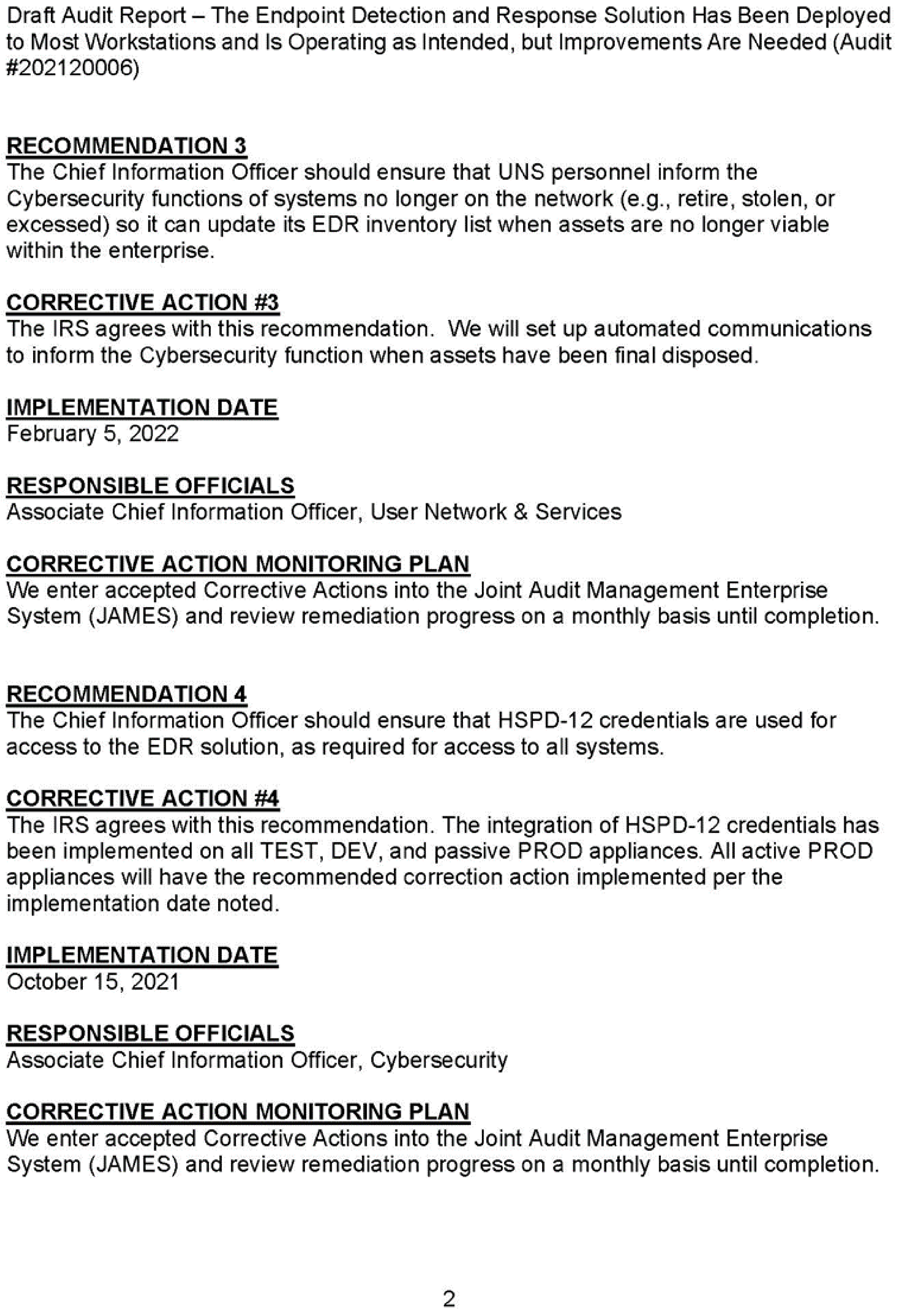
RECOMMENDATION 2
The Chief Information Officer should ensure that the EDR solution is deployed on all workstations that will be brought online and used for IRS business prior to being issued to users.

CORRECTIVE ACTION #2
The IRS agrees with this recommendation. We will integrate [redacted] into the workstation build process so that the EDR solution is installed on newly built workstations, as well as workstations being re-imaged.

IMPLEMENTATION DATE
August 15, 2022

RESPONSIBLE OFFICIALS
Associate Chief Information Officer, User Network & Services

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



Draft Audit Report – The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating as Intended, but Improvements Are Needed (Audit #202120006)

RECOMMENDATION 3
The Chief Information Officer should ensure that UNS personnel inform the Cybersecurity functions of systems no longer on the network (e.g., retire, stolen, or excessed) so it can update its EDR inventory list when assets are no longer viable within the enterprise.

CORRECTIVE ACTION #3
The IRS agrees with this recommendation. We will set up automated communications to inform the Cybersecurity function when assets have been final disposed.

IMPLEMENTATION DATE
February 5, 2022

RESPONSIBLE OFFICIALS
Associate Chief Information Officer, User Network & Services

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

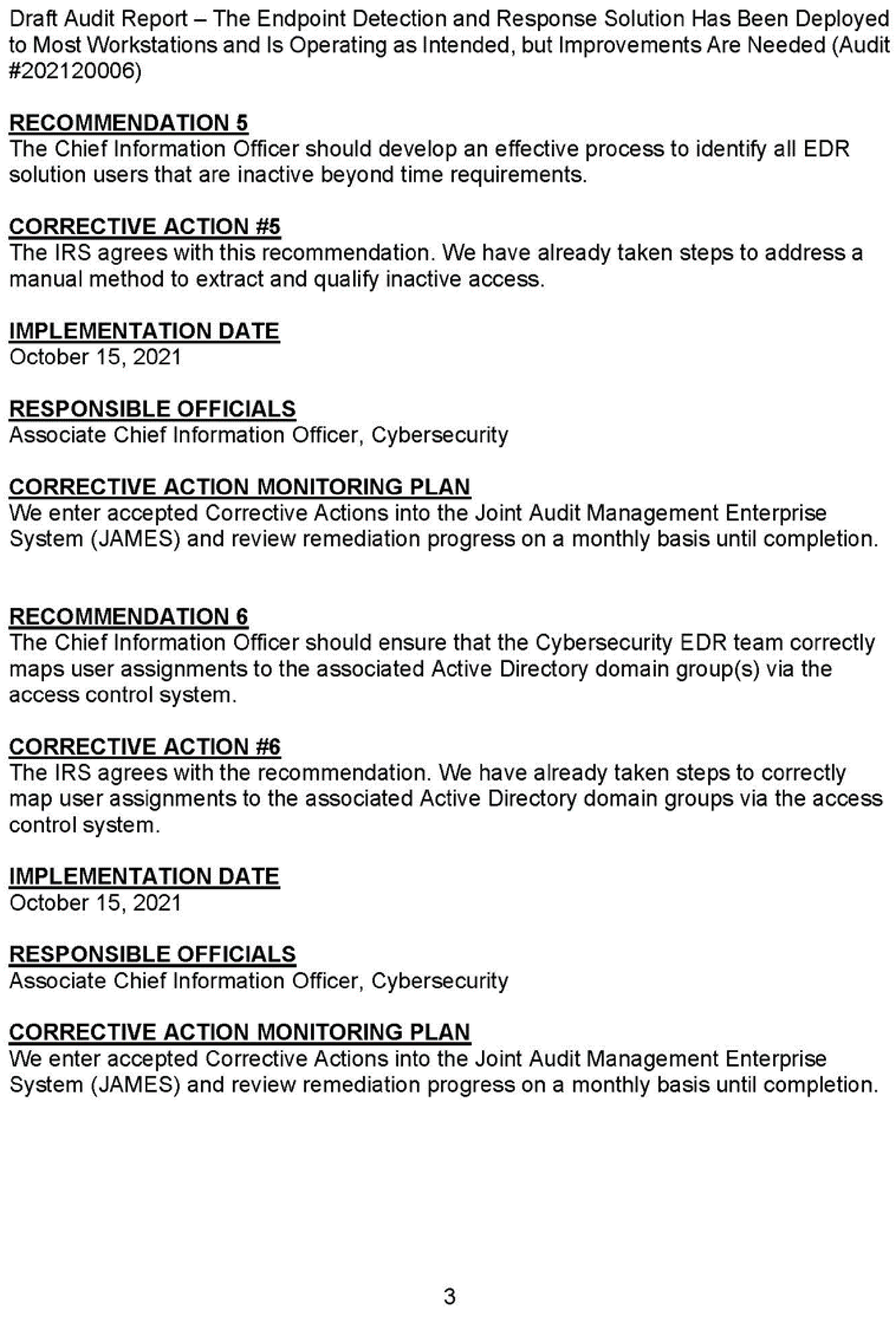
RECOMMENDATION 4
The Chief Information Officer should ensure that HSPD-12 credentials are used for access to the EDR solution, as required for access to all systems.

CORRECTIVE ACTION #4
The IRS agrees with this recommendation. The integration of HSPD-12 credentials has been implemented on all TEST, DEV, and passive PROD appliances. All active PROD appliances will have the recommended correction action implemented per the implementation date noted.

IMPLEMENTATION DATE
October 15, 2021

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 review remediation progress on a monthly basis until completion.



RECOMMENDATION 5

The Chief Information Officer should develop an effective process to identify all EDR solution users that are inactive beyond time requirements.

CORRECTIVE ACTION #5

The IRS agrees with this recommendation. We have already taken steps to address a manual method to extract and qualify inactive access.

IMPLEMENTATION DATE

October 15, 2021

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 review remediation progress on a monthly basis until completion.

RECOMMENDATION 6

The Chief Information Officer should ensure that the Cybersecurity EDR team correctly maps user assignments to the associated Active Directory domain group(s) via the access control system.

CORRECTIVE ACTION #6

The IRS agrees with the recommendation. We have already taken steps to correctly map user assignments to the associated Active Directory domain groups via the access control system.

IMPLEMENTATION DATE

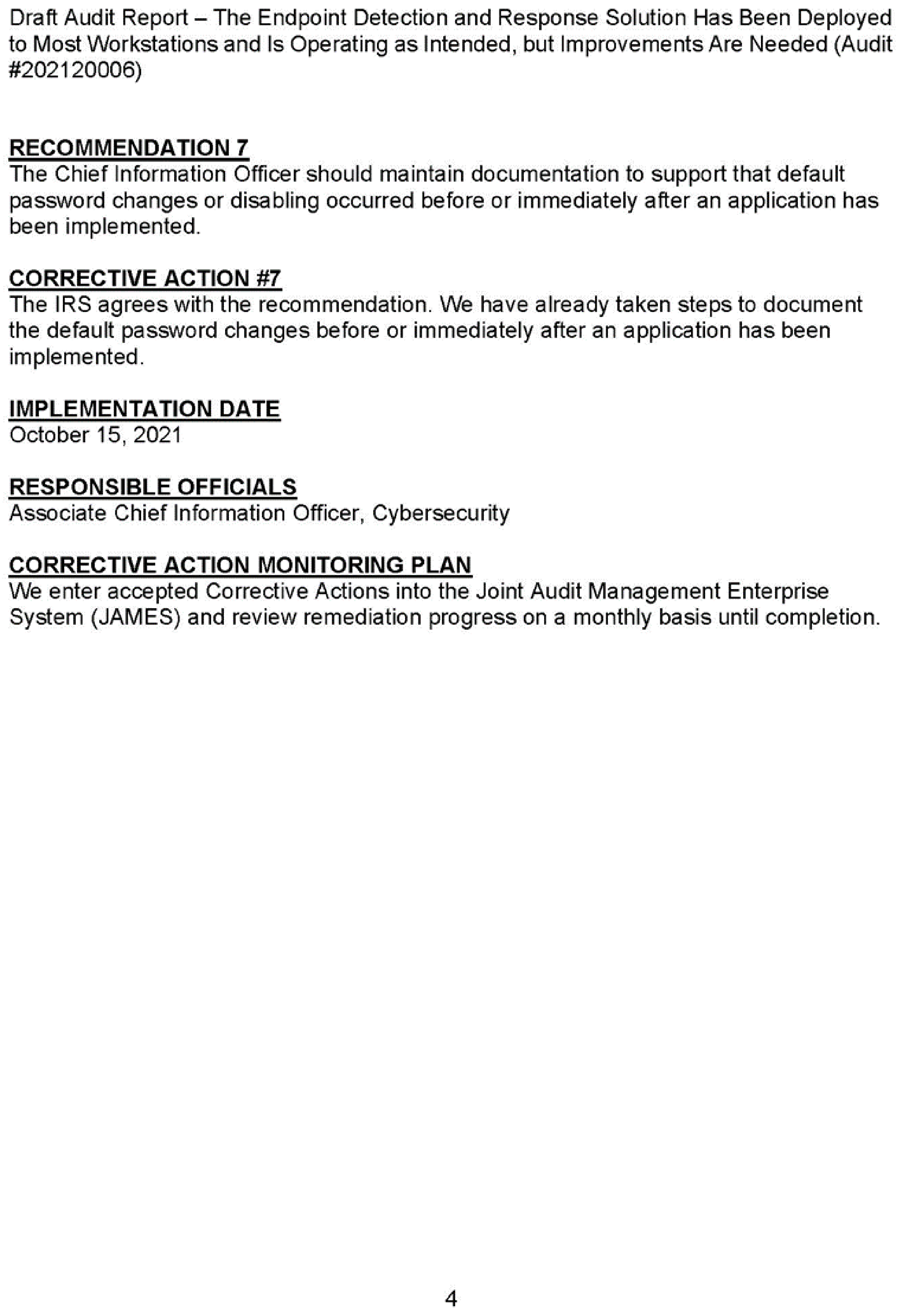
October 15, 2021

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 review remediation progress on a monthly basis until completion.



Draft Audit Report – The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating as Intended, but Improvements Are Needed (Audit #202120006)

RECOMMENDATION 7
The Chief Information Officer should maintain documentation to support that default password changes or disabling occurred before or immediately after an application has been implemented.

CORRECTIVE ACTION #7
The IRS agrees with the recommendation. We have already taken steps to document the default password changes before or immediately after an application has been implemented.

IMPLEMENTATION DATE
October 15, 2021

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 review remediation progress on a monthly basis until completion.

Appendix IV

Glossary of Terms

Term	Definition
Active Directory	A Microsoft Corporation software system for administering and securing computer networks. It manages the identities and relationships of computing resources that comprise a network. It enables administrators to assign enterprise-wide policies, deploys programs to many computers, and applies critical updates to an entire organization simultaneously from a central, organized, accessible database. It simplifies system administration and provides methods to strengthen and consistently secure computer systems.
Appliance	A computing device that provides predefined services and has its underlying operating software hidden beneath an application specific interface.
Application Program Interface	A set of routines, protocols, and tools referred to as "building blocks" used in business application software development.
Bloodhound Scanner	An open-source application used for analyzing security of Active Directory domains. The tool performs data ingestion from Active Directory domains and highlights the potential for escalation of rights in Active Directory domains, thus uncovering hidden or complex attack paths that can compromise the security of a network.
Defense In-Depth	Information security strategy integrating people, technology, and operational capabilities to establish variable barriers across multiple layers and dimensions of the organization.
Embedded Systems	Some combination of computer hardware and software, either fixed in capability or programmable, that is designed for a specific function(s) within a larger system. Embedded systems are computing systems, but they can range from having no user interface to complex graphical user interfaces, such as in mobile devices.
Endpoint Detection and Response	A set of cybersecurity tools that are designed to detect and remove any malware or any other form of malicious activity on a network.
Filing Season	The period from January 1 through mid April when most individual income tax returns are filed.
Host-Based Intrusion Detection System	Monitors a computer system to detect an intrusion or violation of the system's security policies and responds by logging the activity and notifying the designated authority. This tool has the ability to monitor key system files and any attempt to overwrite these files.
In Use	Reflects the service date when the asset inventory record was changed to reflect that the asset was in use. In addition, the term is historically set as a financial qualification to indicate an asset was being used in some capacity by the IRS organization and not as an indication of it being on the network.

Term	Definition
Integrated Submission and Remittance Processing	A system that converts paper tax return and information documents and remittances received by the IRS into perfected electronic records of taxpayer data.
Knowledge Incident/ Problem Service Asset Management System	An application that maintains the complete IRS inventory of information technology and non–information technology assets, computer hardware, and software. It is also the reporting tool for problem management with all IRS-developed applications.
Malware	Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. It can be a virus, worm, Trojan horse, or other code-based entity that infects a host.
Nation-State Attacker	An entity operating on behalf of a recognized government with the characteristics of sovereignty, access, and money.
Online 5081 System	An IRS 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.
Penetration Testing and Code Analysis	Enables application security from the inside out and to improve the IRS's security posture against internal and external threats.
Powershell®	A task-based, command-line shell and scripting language built on .NET that helps system administrators and power users rapidly automate tasks that manage operating systems and processes.
Privileged Account	An account with set "access rights" for certain users on a given system. Sometimes referred to as system or network administrative accounts.
Public Key Infrastructure	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Ransomware	An ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.
[redacted]	[redacted].
Service Center Recognition Image Processing System	A data capture, management, and storage system that uses high-speed scanning and digital imaging technology to process tax documents.

Term	Definition
Software Agent	Offers various benefits to end users by automating repetitive tasks. The basic concepts related to software agents are 1) they are invoked for a task, 2) they reside in "wait" status on hosts, 3) they do not require user interaction, 4) they run status on hosts upon starting conditions, and 5) they invoke other tasks including communication.
Splunk	This network traffic, database, and analytics tool is an industry standard technology used to analyze the streams of machine data generated by information technology systems and technology infrastructure in order to improve both insider threat detection and application troubleshooting.
Symantec	The company produces software for security, storage, backup, and availability and offers professional services to support its software.
Two-Factor Authentication	A method of confirming a user's claimed identity by using a combination of two different components. These components may be something that the user knows, something that the user possesses, or something that is inseparable from the user.

Appendix V

Abbreviations

CSIRC	Computer Security Incident Response Center
EDR	Endpoint Detection and Response
HSPD-12	Homeland Security Presidential Directive-12
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
UNS	User and Network Services

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

(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.