TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Bring Your Own Device Program's Security Controls Need Improvement

September 12, 2019

Reference Number: 2019-20-046

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.

<u>Redaction Legend</u>:
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions

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.

THE BRING YOUR OWN DEVICE PROGRAM'S SECURITY CONTROLS NEED IMPROVEMENT

Highlights

Final Report issued on September 12, 2019

Highlights of Reference Number: 2019-20-046 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The IRS implemented the Bring Your Own Device (BYOD) program to allow its employees to access work resources using their personal mobile devices. Due to their small size, mobile devices can be easily lost or stolen. When that occurs, IRS data on the device can be subject to unauthorized access and the device itself can be used as an avenue to attack IRS systems. The risk is high because various systems and databases managed by the IRS contain significant amounts of tax data and Personally Identifiable Information.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the management and security of the BYOD program to ensure that data are protected while maintaining program cost efficiencies.

WHAT TIGTA FOUND

The BYOD program enhanced security by upgrading to a newer platform. The IRS also completed a cost-benefit analysis that showed reduced costs and a potential increase in productivity due to the BYOD program.

However, TIGTA identified significant vulnerabilities within the BYOD program. For example, the risk of data leakage with personally owned iPhones® is increased because iPhones enable the screenshot functionality, *******2****** **************************2**************************** **************************2**************.

BYOD servers contain critical and high-risk vulnerabilities, such as **************2************* **************************2**************************** **************************2***********. Of the 68 critical and high-risk vulnerabilities identified in one month, 18 (26 percent) were classified as easily exploitable.

TIGTA also identified audit log issues, such as not maintaining change logs to capture system administrator actions and not reviewing application logs. In addition, BYOD program guidelines and procedures need clarification on maintaining and reviewing application logs, reporting lost or stolen devices, and wiping a lost or stolen device's application data as well as updating baseline configuration documentation and educating users on malware prevention. Lastly, the BYOD program did not enforce required annual security training for participants.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS identify a viable solution or take mitigation actions to prevent data leakage from personally owned iPhones; consider disapproving employees with Personally Identifiable Information and Internal Revenue Code Section 6103 violations from participating in the program; and ensure that vulnerabilities on BYOD servers are timely remediated, application audit logs are maintained and reviewed, and application change logs are created, and all BYOD program participants complete the required security training annually. TIGTA also recommended that BYOD program guidelines and procedures be updated regarding configuration baselines, education on malware prevention, reporting lost or stolen BYOD program devices, tracking and wiping application data, and maintaining and reviewing audit logs.

In its response, IRS management agreed with all seven recommendations. The IRS plans to implement solutions or mitigations to the screen capture function on BYOD program devices and strengthen the participant approval process. The IRS also agreed to timely remediate BYOD server vulnerabilities, and to create, review, and retain both application change and audit logs. In addition, it will update policies and guidelines to include malware prevention awareness, the reporting and wiping of data from lost or stolen devices, and the requirement that BYOD program participants complete security awareness training annually.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 12, 2019

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Bring Your Own Device Program's Security Controls Need Improvement (Audit # 201820009)

This report presents the results of our review to evaluate the management and security of the Bring Your Own Device program to ensure that data are protected while maintaining program cost efficiencies. 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 Internal Revenue Service Resources.

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

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

Table of Contents

Appendices

Abbreviations

BYOD	Bring Your Own Device
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
TIGTA	Treasury Inspector General for Tax Administration
2	***********2***********

Background

The devices' mobile nature makes them much more likely to be lost or stolen, so their data are at increased risk of compromise.

The National Institute of Standards and Technology[1] (NIST) defines mobile devices as a portable computing and communications device with information storing capability. Some examples are smartphones, tablets, and laptops. From a business perspective, mobile devices allow organizations to provide their employees with the means to work and communicate away from the traditional office and workstation environment. However, due to their small size, mobile devices can be easily lost or stolen. When that occurs, two things are at risk. First, the content held on the mobile device itself can be subject to unauthorized access. Second, and perhaps more important, mobile devices represent an avenue for hackers to attack systems of the organization.

For organizations like the Internal Revenue Service (IRS), these risks are especially high because the various systems and databases managed by the IRS contain significant amounts of unclassified but sensitive data, such as tax return information and Personally Identifiable Information. If these systems are compromised, they could adversely affect the IRS's ability to operate its systems, protect its assets and employees, and maintain public trust for American taxpayers. From the taxpayer's perspective, this kind of incident could also be used to compromise an individual's financial wellbeing, privacy, or identity. Threats can come from advanced nation-state attacks to organized groups of criminals, using advanced hacking techniques, to the simple theft of mobile phones. Because of this landscape, organizations must protect their mobile devices and the devices of employees participating in a Bring Your Own Device (BYOD) program against unauthorized access and configure the devices' settings to prevent excessive access into an organization's network.

The IRS's BYOD program allows registered users to access select IRS applications and data through their personal mobile devices using secure managed mobile applications provided by the program. The IRS relies on a combination of educating users on their responsibilities and a layered set of security features implemented by the BYOD program mobile service platform. These features include:

- Required user security training prior to participation in the program.
- Encryption of communications between the secure mobile application and IRS systems.
- Mutual two-way authentication of connections.

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

- Automated detection of jailbroken or rooted devices.
- Automated detection of unverified third-party applications.

In September 2010, the IRS began a proof of concept for the BYOD program to validate the technical feasibility of allowing mobile devices onto its network. By May 2013, the IRS had 460 participants with 519 devices registered in the program. In June 2016, the IRS decided to move forward and expand the program as the result of a cost-benefit analysis. In September 2018, the Information Technology organization's User and Network Services function upgraded the BYOD program platform from the Blackberry® Good for Enterprise system to the *******************2******************* system. This upgrade was completed by November 30, 2018. During our review, users were in the process of transitioning to the new system. As of March 2019, 1,283 current BYOD program users have registered in the ********2******** application.

This review was performed at the Washington, D.C.; Atlanta, Georgia; New Carrollton, Maryland; Lee's Summit, Missouri; and Nashville, Tennessee, offices in the Information Technology organization's User and Network Services, Enterprise Operations, and Cybersecurity functions during the period August 2018 through May 2019. 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. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Overall, we found that the BYOD program continues to make improvements to enhance security in a number of key areas. For example, prior to the start of our audit, the IRS did not have a good definition of an "active" user and could not provide a definitive number of users in the system. During the audit, BYOD program management took immediate steps to correct this deficiency, and the IRS has defined what constitutes an active user and is accurately determining the number of current participants. Furthermore, the BYOD program has been upgraded to a new system and has implemented other changes. For example:

- The upgraded BYOD Central website allows user feedback, encourages employee interest, and requires security training prior to participation.
- *******************2*******************.
- The Mobile Voice Access program allows BYOD program participants to mask their phone number if they need to use their BYOD program device for work calls.
- Work e-mail notifications that display on the BYOD program device do not show the sender's name to maintain confidentiality of the sender until the device is accessed.

We also determined that the IRS had varying degrees of success when implementing planned corrective actions from the prior Treasury Inspector General for Tax Administration (TIGTA) audit report on the BYOD program.[2] For example, we cited concerns that the IRS had not developed a complete cost-benefit analysis to justify the program. The IRS Chief Technology Officer agreed to the recommendation, but the IRS did not act on the recommendation, as the program was a technical demonstration and not a pilot. However, in March 2014, the IRS had a cost-benefit analysis performed by a contractor that showed reduced costs and a potential increase in productivity, resulting in a decision to move forward with the program. As such, we believe that the IRS addressed our recommendation. We also found that the IRS implemented planned corrective actions on audit trails and refresher training on BYOD program risks, but we identified concerns over both of those areas, which we present in this report.

We identified significant vulnerabilities in the BYOD program. For example, a data leakage concern exists with user configurations on personally owned mobile devices, which can allow the user to take a screenshot of information displayed on the device, *******2********. We also found that the IRS is not fixing critical and high-risk vulnerabilities and is not maintaining and reviewing application logs on BYOD program systems. Finally, BYOD program management cannot ensure that BYOD program participants have completed the annual security

[2] TIGTA, Ref. No. 2013-20-108, *Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot* (Sept. 2013).

risk awareness training as required or that lost or stolen BYOD program devices were properly wiped to remove Personally Identifiable Information and taxpayer data from the devices.

BYOD Program Users With Personally Owned iPhones Have Screenshot Capabilities That Could Allow Data Leakage to Occur

During our review, we interviewed BYOD program users and asked them to test various functions on their device. As a result, we identified a security vulnerability exclusive to the iPhone®. We tested 23 iPhones and determined that all 23 devices had the capability to take a screenshot of the information on the display and save the image on the device. For example, **************************************2*************************************
**************************************2*************************************
**************************************2*************************************
**************************************2*************************************
********2********. To our knowledge, this capability has been in effect for more than three years. The IRS has deactivated the screenshot feature on its Government-issued iPhones.

Personally owned BYOD iPhones cannot be configured to disallow the screenshot function without completely rendering the function disabled for all of the device applications. The user is essentially the administrator over the device and all of its features and can allow the screenshot function to work.

The Internal Revenue Manual (IRM)[3] states that BYOD program participants shall not use the screenshot function on their mobile device while logged into the IRS-approved mobile access solution. The IRS is relying on policy alone to ensure the employee's compliance, but in our opinion, this rule of behavior restriction is not enough to deter a BYOD program user from taking advantage of this capability because there is no way to monitor or detect when this function is used.

To further illustrate the risk for potential data leakage, we identified nine BYOD program participants who had previous Personally Identifiable Information e-mail violations logged against them. Seven of the nine users had iPhones. Although we could not determine what method was used to access the e-mail, these employees could be considered a higher threat risk and may take advantage of this vulnerability and further violate disclosure rules while remaining undetected.

When an employee wants to participate in the BYOD program, the employee must go through the Online 5081 process to request participation in the program. Through this process, the employee's manager must approve participation in the program. This managerial decision point is an opportune time to consider disapproving the employee's request to participate in the BYOD

[3] IRM 10.8.26, *Information Technology Security, Government Furnished and Personally Owned Mobile Device Security Policy* (Feb. 2017).

program if the employee has Personally Identifiable Information or Internal Revenue Code Section (§) 6103[4] violations.

Recommendations

To reduce the risk to the BYOD program, the Chief Information Officer should:

Recommendation 1: Identify a viable solution or take mitigation actions to prevent data leakage through the screen capture function on personally owned iPhones in the BYOD program.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will complete a risk assessment of the finding and implement solutions or mitigations, as identified, to address the risk.

Recommendation 2: Coordinate with other IRS offices, such as Labor Relations, to ensure that the employee's manager considers employee Personally Identifiable Information and Internal Revenue Code § 6103 violations prior to approving participation.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has policies in place for managers for approving employee participation and will strengthen the policies to include additional guidance to managers on the approval process.

BYOD Servers Have Critical-Risk and High-Risk Vulnerabilities

The IRS currently scans the BYOD servers for vulnerabilities on a weekly basis. We analyzed the January through October 2018 vulnerability scans. The scans from January through July 2018 showed little to no high-risk vulnerabilities. However, the August through October 2018 scans had an increase in critical-risk and high-risk vulnerabilities. These vulnerabilities appear on the same servers in two or more consecutive months, which indicates that the IRS is not timely remediating the critical-risk or high-risk vulnerabilities. According to the IRM[5] guidelines, critical-risk and high-risk vulnerabilities are to be patched within 30 calendar days. The software vendor regularly posts vulnerabilities with suggested corrective actions to assist in remediating the vulnerabilities. Figure 1 shows the number of critical-risk and high-risk vulnerabilities for each of the three months.

[4] Internal Revenue Code § 6103, *Confidentiality and disclosure of returns and return information.*

[5] IRM 10.8.50, *Information Technology Security, Servicewide Security Patch Management* (Apr. 2016).

Figure 1: Critical-Risk and High-Risk Vulnerabilities on the BYOD Servers for August Through October 2018

Vulnerability	August 2018	September 2018	October 2018
Critical-Risk	28	27	29
High-Risk	38	29	39
Totals	66	56	68

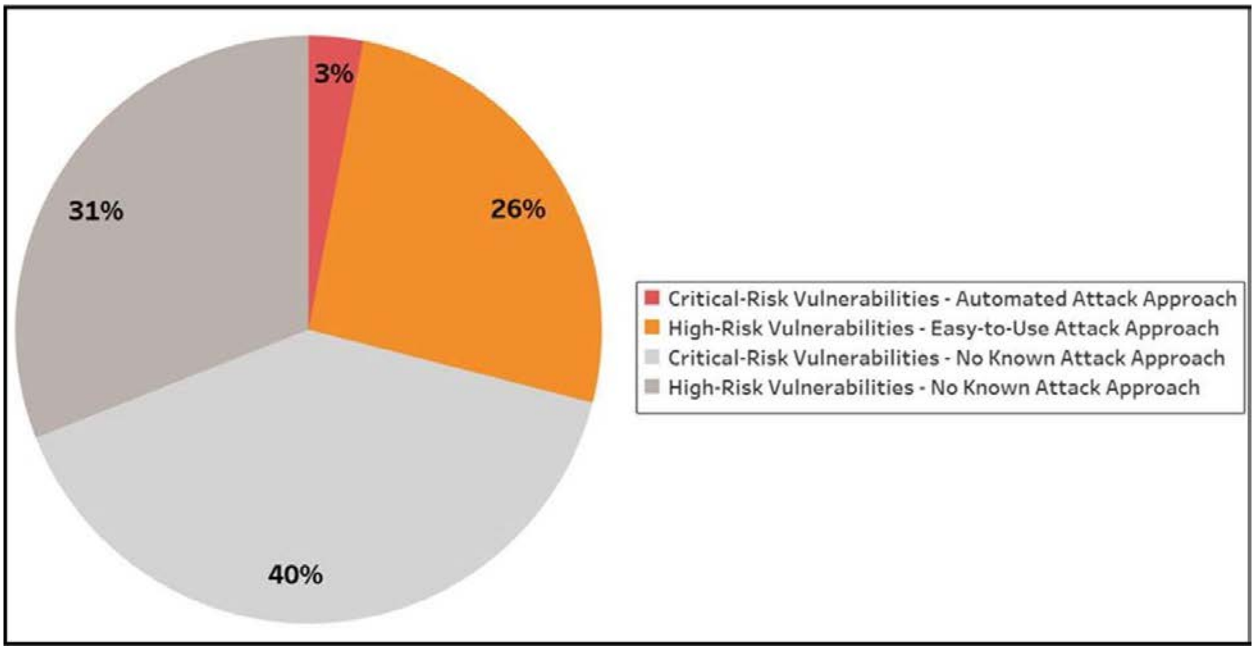
Source: TIGTA analysis of BYOD servers.

We discussed our results with Enterprise Operations function Secure Enterprise Messaging System organization officials, who are responsible for the BYOD servers. Normally, they receive the scans from the Cybersecurity function on a monthly basis; however, they did not recognize the scans that were provided to us and were unaware of the critical-risk and high-risk vulnerabilities. Secure Enterprise Messaging System organization officials stated that they would take a closer look at their communication processes with the Cybersecurity function to ensure that scan reports are being shared.

Hackers use different attack approaches to exploit vulnerabilities. Many of the vulnerabilities are public knowledge, making them exploitable to hackers or persons with malicious intent. Public availability of an easy-to-use attack approach increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability and the risk to the system. The risk rating levels from the ****2**** scans used by the IRS take into consideration the likelihood of an exploit based on the availability and skill level of exploit methods and tools. In other words, known vulnerabilities may have a known easy-to-use or automated attack approach, making the vulnerability extremely likely to be exploited and thus increasing the risk level of the vulnerability. *******************2******************** **************************************2************************************* **************************************2************************************* **************************************2************************************* **************2***********.

**************************************2************************************* **************************************2*******************. Figure 2 shows the percentage of attack approaches for the IRS's critical-risk and high-risk vulnerabilities in October 2018, which had the highest number of vulnerabilities. For instance, 18 (26 percent) high-risk vulnerabilities had the "easy-to-use" attack approach and two (3 percent) had an "automated" attack approach. The remainder did not have a "known" attack approach.

Figure 2: Types of Possible Attack Approaches for Exploiting Vulnerabilities on BYOD Servers in October 2018



Source: TIGTA analysis of BYOD servers for October 2018.

The IRM[6] states that the IRS must remediate the critical-risk and high-risk vulnerabilities within 30 calendar days of discovery. Allowing critical-risk and high-risk vulnerabilities to remain on the servers could potentially put BYOD servers at risk of intrusion or data loss.

Recommendation

Recommendation 3: The Chief Information Officer should ensure that the IRM requirement is met and vulnerabilities found on BYOD servers are timely remediated.

> ***Management's Response:*** The IRS agreed with this recommendation. Following the audit, IRS officials completed an analysis on the vulnerability reports and took immediate actions to confirm remediation on several findings. The IRS will continue to monitor vulnerabilities on the BYOD system and deploy remediations in accordance with the IRM requirement.

[6] IRM 10.8.50 (Apr. 2016).

Retention and Review of Application Audit Logs and Application Change Logs Do Not Meet Standards

An audit trail is a historical record of system activity and processes by both the system itself and the applications residing on the system as well as user activity of the system and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance issues, and flaws in applications. For example, audit trails can provide a means to reconstruct events when a system outage occurs, promote individual accountability to ensure that users are accessing the systems for their intended purposes, and track changes to system settings, which might be used to detect unscheduled or unauthorized changes to the system. In addition, application configuration change logs are audit trail records that capture activities before and after changes are made to the baseline configurations for information technology products, including those made to remediate vulnerabilities. Because of the useful nature of these records, the IRM[7] requires IRS personnel to maintain and review electronic audit logs.

Application audit log files are neither retained nor reviewed as required

In our September 2013 audit report[8] on the BYOD program, we reported that IRS management agreed to ensure that the existing IRS policy related to audit trails is followed, including retaining the audit trails for at least 90 days and reviewing the audit trails daily to identify anomalies that could indicate unauthorized access attempts or security breaches. The IRS's planned corrective action was to retain three-year "rolling" audit log files.

Based on the completion of this corrective action, we requested the three-year log files for the Good for Enterprise Application. However, the IRS could not provide current three-year log files as it had stopped logging data in January 2016. The IRS was unaware that the application log files had stopped logging data until we requested this information. We concluded that, if the log files had been reviewed on a regular basis, the IRS would have known that its BYOD servers had stopped logging prior to our request.

We also requested the application audit logs from the **2** BYOD servers for the migration period of September through November 2018. However, the IRS stated that it does not have the server capacity to retain the logs for longer than two weeks. The current process requires that the administrators of the Secure Enterprise Messaging Systems group receive notification when the disk capacity on the BYOD server reaches its 90 percent threshold. When that occurs, a member of the group deletes the log files. As a result, approximately, only two weeks of audit logs are retained from BYOD servers. Therefore, even though the review of BYOD program audit log files did not show any risk to the BYOD systems, we only analyzed 11 days of data before the

[7] IRM 10.8.1, *Information Technology Security Policy and Guidance* (July 2015).
[8] TIGTA, Ref. No. 2013-20-108, *Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot* (Sept. 2013).

logs were deleted. The IRS does not archive these log files because they do not have the server capacity, so there is no way to recover this deleted information.

**************************************2*************************************
**************************************2*************************************
**************************************2*************************************
**********2*********.

NIST guidance[9] states that the organization should retain audit records for the organization's defined time period consistent with its records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. However, the IRM[10] does not define a specific time period in accordance with NIST guidance. NIST guidance[11] also states that, to meet data retention requirements, organizations might need to keep copies of log files for a longer period of time than the original log sources can support, which necessitates establishing log archival processes.

By not reviewing log files, the IRS cannot detect suspicious activities or inappropriate accesses on its BYOD servers. Without maintaining log files longer than two weeks, the IRS may have a very difficult time investigating questionable activities or potential incidents after two weeks have passed. ***************************2*************************************
**************************************2*************************************
**************************************2*************************************
*******************2****************.

An application change log is not created

An application change log registers any changes made to the configuration of the system, as well as who made them and when they were made. We requested the change log for the six-month period of February through July 2018 for the BYOD program application configurations. However, the IRS stated that it does not maintain a change log for administrator configuration changes to the BYOD program *2* application. The administrators never created a change log for the BYOD program.

We determined that the IRS does not follow the IRM[12] change management policy when dealing with the application's system configuration. According to NIST guidance,[13] configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to

[9] NIST, NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).
[10] IRM 10.8.1 (July 2015).
[11] NIST, NIST Special Publication 800-92, *Guide to Computer Security Log Management* (Sept. 2006).
[12] IRM 10.8.1 (July 2015).
[13] NIST, NIST Special Publication 800-53, Revision 4 (Apr. 2013).

baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology, unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Auditing of any configuration changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes.

Without the application change log, there is no record of the events pertaining to any changes made to configurations, including what was changed in the system. Any misconfiguration that might cause an outage or potential data compromise or data loss cannot be fully diagnosed to ensure that it does not occur again.

Recommendations

The Chief Information Officer should:

Recommendation 4***:*** Ensure the retention of BYOD program application audit logs for the appropriate period and periodic review of the application audit logs by an independent source.[14]

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will complete an assessment to determine the capacity and resource requirements to further implement the recommendation for the retention and periodic reviews of the application audit logs by an independent source. The IRS will implement the solutions or mitigations to meet the requirement contingent upon budgetary, technical, and resource allocations.

Recommendation 5: Ensure the creation and review of an application change log for BYOD program application configuration changes.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will create and review an application change log for BYOD program configuration changes.

BYOD Program Procedures and Guidelines Need Updating

NIST guidance[15] states that, when planning mobile device security policies and controls, organizations should assume that mobile devices will be acquired by malicious parties who will attempt to recover sensitive data either directly from the devices themselves or indirectly by using the devices to access the organization's remote resources.

A mobile device security policy should define which types of the organization's resources may be accessed via mobile devices, which types of mobile devices are permitted to access the organization's resources, the degree of access that various classes of mobile devices may have,

[14] See Recommendation 6 for updating guidelines and procedures for retention and review of audit logs.
[15] NIST, NIST Special Publication 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (June 2013).

and how provisioning should be handled. It should also cover how the organization's centralized mobile device management servers are administered, how policies in those servers are updated, and all other requirements for mobile device management technologies.

During our review, we compared the Federal requirements for BYOD programs against IRS BYOD program policy. IRS BYOD program policy is predominantly in IRM 10.8.26,[16] which was last updated February 28, 2017. We identified the following areas in which IRS BYOD program policy is silent, particularly in comparison to the Federal requirements:

- BYOD program user procedures for downloading an antivirus software to the mobile device.
- Procedures for manually wiping a lost or stolen BYOD program participant's application data.

We also identified IRM policy, procedures, and guidelines that were not clear or needed updating to address the following:

- How and when to report lost or stolen BYOD program mobile devices to the Computer Security Incident Response Center.
- How long to retain application audit logs and how often to review these logs because the IRM[17] section that defined this information is now obsolete.
- Documentation for mobile device baseline configurations[18] (the last updates were from December 2015 and January 2016).

Proactive user procedures can help deter malware

Mobile malware protection is critical. At its most basic, mobile antivirus software performs malware scans to identify and prevent infections. However, solutions have become increasingly sophisticated, such as remote monitoring, device lock, alarm, and wipe as well as Global Positioning System capability to locate lost or stolen devices.

We identified only two of 39 devices that had an antivirus software downloaded as extra security. The IRS ***************************2*********************************. However, *2* configurations for the BYOD program prevent users from installing third-party applications not distributed by Apple® and Android™ stores.

We believe that the BYOD program user should be educated on an antivirus software as well as other techniques that are good proactive measures against malware. For instance, without

[16] IRM 10.8.26 (Feb. 2017).
[17] IRM 10.8.3, *Information Technology Security, Audit Logging Security Controls* (Apr. 2017).
[18] Referred to in IRM 10.8.26, Exhibits 1 and 2 (Feb. 2017).

antivirus software, a user could unknowingly download malware that was contained on a file or application to their device.

Many brands of antivirus software are available, most of which offer similar functionality. NIST guidance[19] recommends configuring antivirus software for the following types of functions:

- Automatically checking for and acquiring updates of signature or data definition files at least daily.
- Monitoring the behavior of common applications, such as e-mail clients, web browsers, file transfer and file sharing programs, and instant messaging software.
- Performing real-time scans of each file as it is downloaded, opened, or executed.
- Handling files that are infected by attempting to disinfect them, which refers to removing malware from within a file, and quarantining them, which means that files containing malware are stored in isolation for future disinfection or examination.

Wiping procedures for lost or stolen devices need clarification

The *2* system remotely wipes, *i.e.*, deletes, the application data if there is no device activity for 30 calendar days. The system also wipes the application data if the device is jailbroken or rooted. A systemic e-mail is generated to notify the BYOD program team of these events. However, we did not identify any local procedures requiring a manual wipe of the device application data if the device was reported lost or stolen or any procedures for tracking manual or systemic application wipes. If mobile devices are lost or stolen and are not wiped of IRS sensitive information, the IRS is at risk of having its data recovered by a malicious party.

We identified two employees who reported their personally owned BYOD program devices lost or stolen to the TIGTA Office of Investigations during January 2017 through December 2018. However, the BYOD program team could not provide a wipe report for that period. As such, we had no assurance that the BYOD program wiped the devices' application data when the devices were reported lost or stolen. These devices could have contained Personally Identifiable Information or taxpayer data.

NIST guidance[20] requires the remote wiping of the device if it is suspected that the device has been lost or stolen. The IRS has the ability to manually wipe the application data when a device is reported lost or stolen. We determined that miscommunication of procedures was part of the cause for the application data not being wiped. The User and Network Services function administrators were under the assumption that BYOD program users' lost and stolen devices were to be reported to the Computer Security Incident Response Center. However, Computer

[19] NIST, NIST Special Publication 800-114, Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security* (July 2016).
[20] NIST, NIST Special Publication 800-124, Revision 1 (June 2013).

Security Incident Response Center officials stated that they only handle Government-furnished lost and stolen devices. We also identified conflicting procedures for reporting lost or stolen BYOD program devices. The BYOD program user agreement as well as the IRS's Breach Response Plan[21] both state to report the device to the Computer Security Incident Response Center. However, the BYOD program training information as well as the BYOD Central website inform the user to fill out a Situation Awareness Management Center report and report the lost or stolen device to the TIGTA Office of Investigations. In addition to this confusion in reporting lost or stolen BYOD program devices, there are no communication procedures to alert the BYOD program to remotely wipe the application data on the lost or stolen device.

The IRS stated that it was in the process of updating the IRM. Since July 2017, the BYOD program has been short-staffed. During this time, it also was planning and implementing the transitioning to BYOD 2.0.

Updating BYOD program security policy ensures that all information technology users within the BYOD program comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organization's boundaries of authority. The IRS should protect its data and control how it is distributed both within and outside the organization.

Recommendation

Recommendation 6: The Chief Information Officer should update BYOD program procedures and guidelines to include:

- Providing malware prevention training to users.
- Updating the documentation for device operating system and technical baseline configurations.
- Maintaining and reviewing application audit logs, specifically time frames for each.
- Clarifying the Computer Security Incident Response Center reporting procedures for a lost or stolen device.
- Informing the BYOD program when a device is lost or stolen so that the application data are remotely wiped.
- Tracking the manual and systemic application data wipes by the BYOD program on a periodic basis.

[21] IRS Breach Response Plan 2.1 (May 2018). The IRS's Breach Response Plan outlines the methodology the IRS uses to categorize breaches of Personally Identifiable Information and determines the appropriate response based on the Office of Management and Budget Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 2017).

Management's Response: The IRS agreed with this recommendation and will complete the following actions:

- Update user training to include malware prevention awareness.
- Update the documentation for device operating system and technical baseline configurations.
- Review and update the procedures and guidelines related to application audit logs, including time frames for each.
- Clarify the Computer Security Incident Response Center reporting procedures for a lost or stolen device.
- Confirm the process to inform the BYOD program when a device is lost or stolen so that the application data are remotely wiped.
- Implement a process to periodically track the manual and systemic application data wipes by the BYOD program.

BYOD Program Security Training Should Be Taken Annually

In our September 2013 audit report[22] on the BYOD program, we recommended that the IRS provide periodic refresher training to BYOD program participants that clearly explains the risks associated with personal mobile devices, how these risks can potentially expose the IRS network to unauthorized accesses and malware, the consequences of such breaches, and how to prevent or reduce the possibility of causing such a security breach. The IRS agreed with our recommendation.

Currently, the BYOD program has a Security Risk Awareness and Guidance presentation that BYOD program applicants must take and acknowledge prior to joining the program. The presentation makes the participant aware of the risks and consequences of using a personally owned device to access Government information. It also informs the participants how to prevent or reduce security breaches.

The IRM[23] was updated in February 2017 to require BYOD program participants to take Operational Security training that provides usage guidelines and vulnerability mitigation techniques for personally owned mobile devices being used to access IRS networks and data. The authorizing official shall verify that each mobile device user completes the required mobile device user training annually.

[22] TIGTA, Ref. No. 2013-20-108, *Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot* (Sept. 2013).
[23] IRM 10.8.26 (Feb. 2017).

We determined that employees were not taking the required annual refresher training because BYOD program management was not enforcing the existing policy and was not following up on employee compliance. In addition, the focus and efforts recently have been to transition the program from the Good for Enterprise system to the *2* system. During our review, BYOD program management stated that they are negotiating implementation of the required annual training to be included on the Enterprise Learning Management System, where the annual training will be enforceable and monitored.

Without annual refresher training, the user may forget the regulations or claim that they were unaware of the security guidance, which can lead to data leakage or expose the IRS network to unauthorized access.

Recommendation

Recommendation 7***:*** The Chief Information Officer should ensure that BYOD program participants complete the security risk awareness training annually and that the authorizing official certifies employee training compliance.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will implement a policy to require BYOD program participants to complete security risk awareness training annually, and the authorizing official will certify employee training compliance.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the management and security of the BYOD program to ensure that data are protected while maintaining program cost efficiencies. To accomplish our objective, we:

I. Followed up on previously reported findings, recommendations, and implemented corrective actions from a prior TIGTA report.[1]

A. Assessed whether a BYOD program pilot cost-benefit analysis was prepared.

B. Reviewed steps taken to ensure that the existing IRS policy related to audit trails is consistently followed.

C. Assessed whether refresher training is provided to BYOD program participants that clearly explains the risks associated with personal mobile devices and how to prevent or reduce the possibility of causing a security breach.

II. Evaluated the process and practices to ensure that BYOD program participants are using their devices in a secure manner.

A. Evaluated the IRS's BYOD program policy for protecting IRS data.

B. Determined if BYOD program users are securing their devices for the BYOD program by interviewing a judgmental sample of various groups of BYOD program participants. The IRS provided us a population of 2,126 devices. From this population, we identified the participants for the associated devices. We then selected a sample[2] of 70 participants with 84 associated devices based on availability in the various locations as well as different work areas, such as management, field, and information technology.

III. Assessed the effectiveness of BYOD program physical controls by evaluating the procedures for protecting IRS data when the device is lost, stolen, or upgraded.

IV. Assessed the effectiveness of preventing third-party applications and mitigating system security weaknesses.

[1] TIGTA, Ref. No. 2013-20-108, *Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot* (Sept. 2013).

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

A. Determined the process for identifying applications that the Information Technology organization has deemed unsafe or not allowed for use on BYOD program devices (third-party applications).

B. Assessed the effectiveness of mitigating system security weaknesses in the BYOD program by determining if vulnerabilities[3] were remediated timely and if the audit trails were retained and reviewed regularly for any anomalies.

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: IRM 10.8.26[4] and NIST Special Publication 800-124, Revision 1.[5] We also determined that other related IRS guidelines for securing personally owned mobile devices, patching vulnerabilities, and reviewing and maintaining audit logs for the BYOD program were relevant. We evaluated these controls by conducting interviews and meetings with the Information Technology organization's User and Network Services, Enterprise Operations, and Cybersecurity functions and reviewing relevant documentation.

[3] See Appendix IV for the glossary of terms.

[4] IRM 10.8.26, *Information Technology Security, Government Furnished and Personally Owned Mobile Device Security Policy* (Feb. 2017).

[5] NIST, NIST Special Publication 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (June 2013).

Appendix II

Major Contributors to This Report

Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Joseph F. Cooney, Audit Manager
Cari Fogle, Lead Auditor
Suzanne Westcott, Senior Auditor
Thomas Martin, Information Technology Specialist

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, User and Network Services
Director, Secure Enterprise Messaging System
Director, Unified Communications
Director, Enterprise Audit Management

Appendix IV

Glossary of Terms

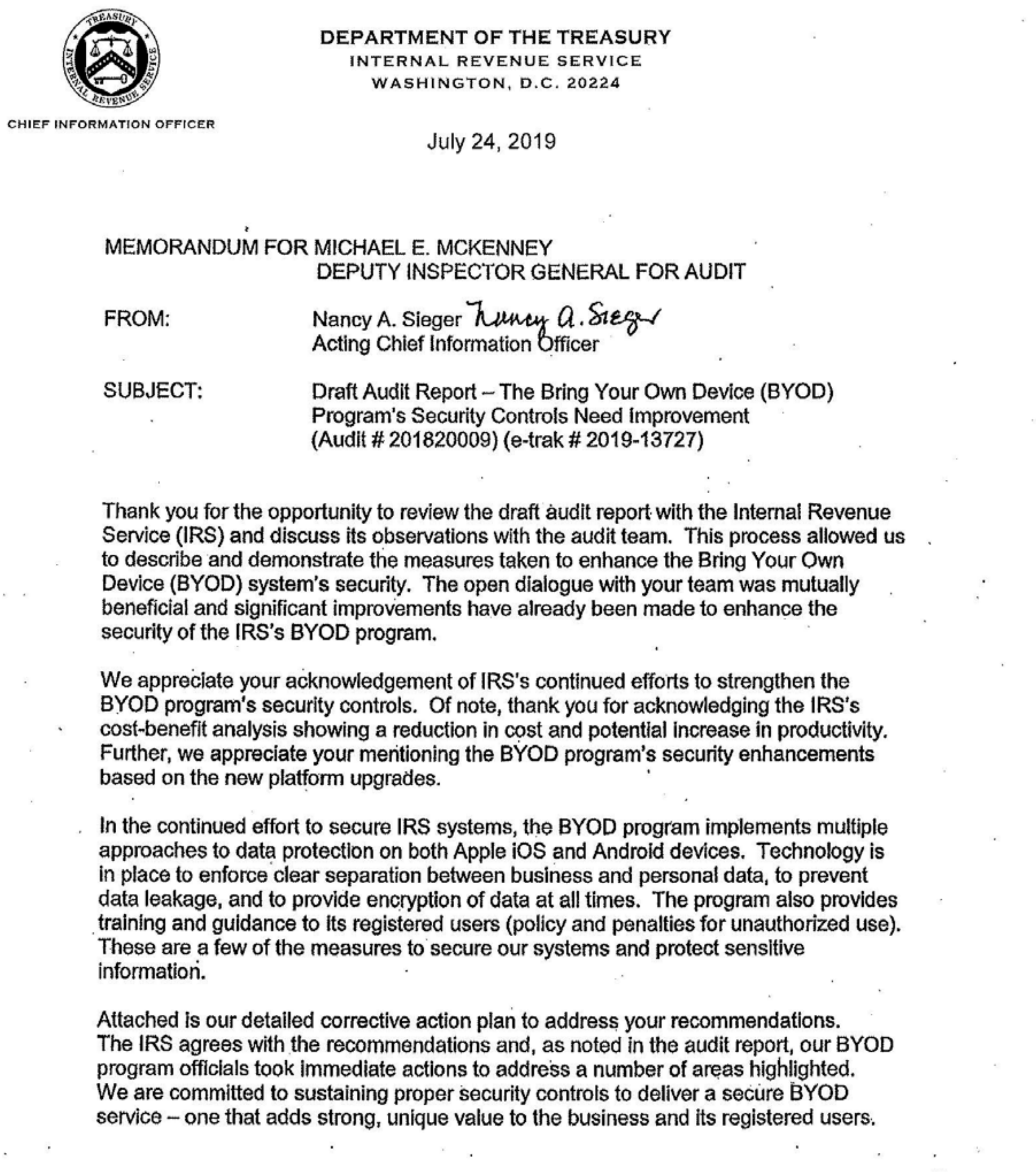
Term	Definition
Antivirus Software	A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.
Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.
Automated Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality using exploit methods that automatically seek vulnerable hosts and exploit the vulnerable application automatically.
*******2*******	************************2************************* ************************2************************* ************************2************************* ************************2************************* ************************2*******************.
Change Log	Audit trail records that capture activities before and after changes are made to the baseline configurations for information technology products, including those made to remediate vulnerabilities. It registers any changes made to the configuration of the system as well as who made them and when they were made.
Computer Security Incident Response Center	Positioned to be proactive in preventing, detecting, and responding to computer security incidents targeting the IRS's enterprise information technology assets. It provides assistance and guidance in incident response and provides a centralized approach to incident handling across the IRS enterprise.
Database	An usually large collection of data organized especially for rapid search and retrieval (as by a computer).
Easy-To-Use Attack	A "point-and-shoot" exploit that requires little or no technical knowledge to achieve a successful attack.

Term	Definition
Enterprise Learning Management System	A learning management system is used for the administration, documentation, tracking, and reporting training, as well as the delivery of e-Learning. The Enterprise Learning Management System is the IRS Learning Management System, which is the system of record for all IRS training.
Jailbroken	An attempt to bypass certain security features built into Apple devices. Jailbreaking allows root access to the operating system and may allow a user to use applications (referred to as apps) besides those in the Apple apps store.
Malware	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Mobile Voice Access	A program that offers a second Government phone line solution for all BOYD program holders. This program allows an employee to use their personal phone and have it appear as their desk phone when making outgoing calls.
Nation-State Attacks	Nation-state attacks, and the threat of them, appear to be evolving. The theory that these state-backed cybercriminals are focused on hacking into military or diplomatic data for competitive intelligence now needs to be broadened to other motivating factors. Nation-state hackers are expanding their targets to not only government institutions, but also businesses and industrial facilities. They are using more sophisticated techniques to disrupt organizations, and their respective countries, by leaking confidential, often sensitive, information.
National Institute of Standards and Technology	Under the Department of Commerce, this organization is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
Online 5081 Application	An application that streamlines the request for adding, deleting, modifying, and resetting passwords for authorized IRS employees, vendors, and contractors as users on IRS applications/systems.

Term	Definition
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, or biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name.
Rooted	A mobile device that has been modified to bypass the built-in restrictions on security, operating system use, *etc*.
Secure Enterprise Messaging System	Outlook Secure Messaging allows you to digitally encrypt e-mail messages and attachments for transmission between IRS e-mail users. Secure Messaging is available to everyone with an Enterprise e-mail account and approved workstation. Secure Messaging is used to encrypt e-mail messages and attachments holding Sensitive But Unclassified information.
Separation of Duties	Control policy according to which no person should be given responsibility for more than one related function.
Situation Awareness Management Center	This center is tasked with documenting all physical security incidents and/or threats Service-wide. The 24/7 operation supports the Facilities Management and Security Services function and the IRS's law enforcement partners to ensure the safety of its employees, facilities, and infrastructure.
Smartphone	A cell phone with built-in applications (apps), access to the Internet, and the ability to add more apps.
*******2*******	*************************2**************************. *************************2************************** *************************2***********************.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
*******2*******	*************************2************************** *************************2************************** *************************2************************** *************************2************************** *************2***********.

Appendix V

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

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

July 24, 2019

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

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

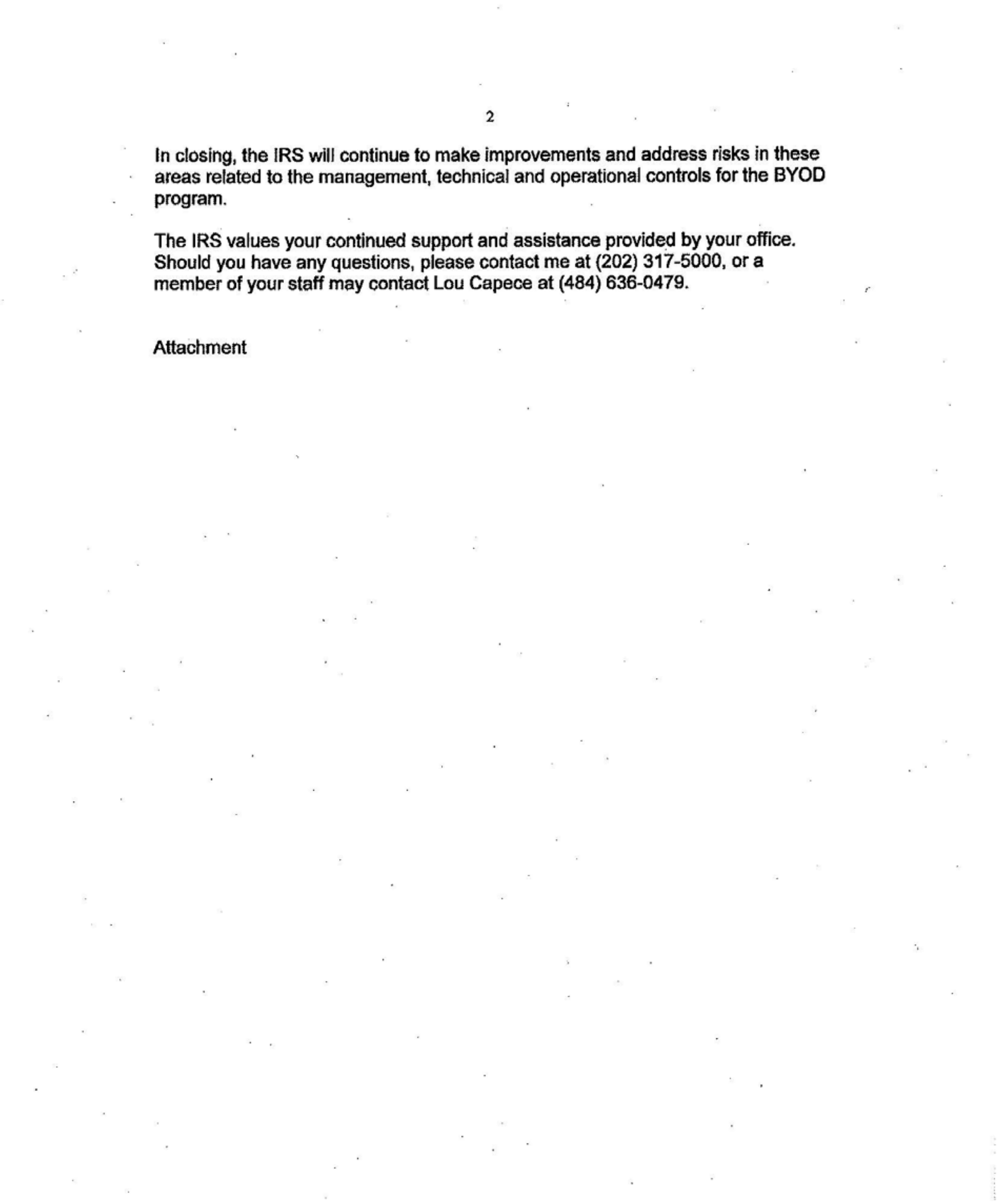
SUBJECT: Draft Audit Report – The Bring Your Own Device (BYOD) Program's Security Controls Need Improvement (Audit # 201820009) (e-trak # 2019-13727)

Thank you for the opportunity to review the draft audit report with the Internal Revenue Service (IRS) and discuss its observations with the audit team. This process allowed us to describe and demonstrate the measures taken to enhance the Bring Your Own Device (BYOD) system's security. The open dialogue with your team was mutually beneficial and significant improvements have already been made to enhance the security of the IRS's BYOD program.

We appreciate your acknowledgement of IRS's continued efforts to strengthen the BYOD program's security controls. Of note, thank you for acknowledging the IRS's cost-benefit analysis showing a reduction in cost and potential increase in productivity. Further, we appreciate your mentioning the BYOD program's security enhancements based on the new platform upgrades.

In the continued effort to secure IRS systems, the BYOD program implements multiple approaches to data protection on both Apple iOS and Android devices. Technology is in place to enforce clear separation between business and personal data, to prevent data leakage, and to provide encryption of data at all times. The program also provides training and guidance to its registered users (policy and penalties for unauthorized use). These are a few of the measures to secure our systems and protect sensitive information.

Attached is our detailed corrective action plan to address your recommendations. The IRS agrees with the recommendations and, as noted in the audit report, our BYOD program officials took immediate actions to address a number of areas highlighted. We are committed to sustaining proper security controls to deliver a secure BYOD service – one that adds strong, unique value to the business and its registered users.

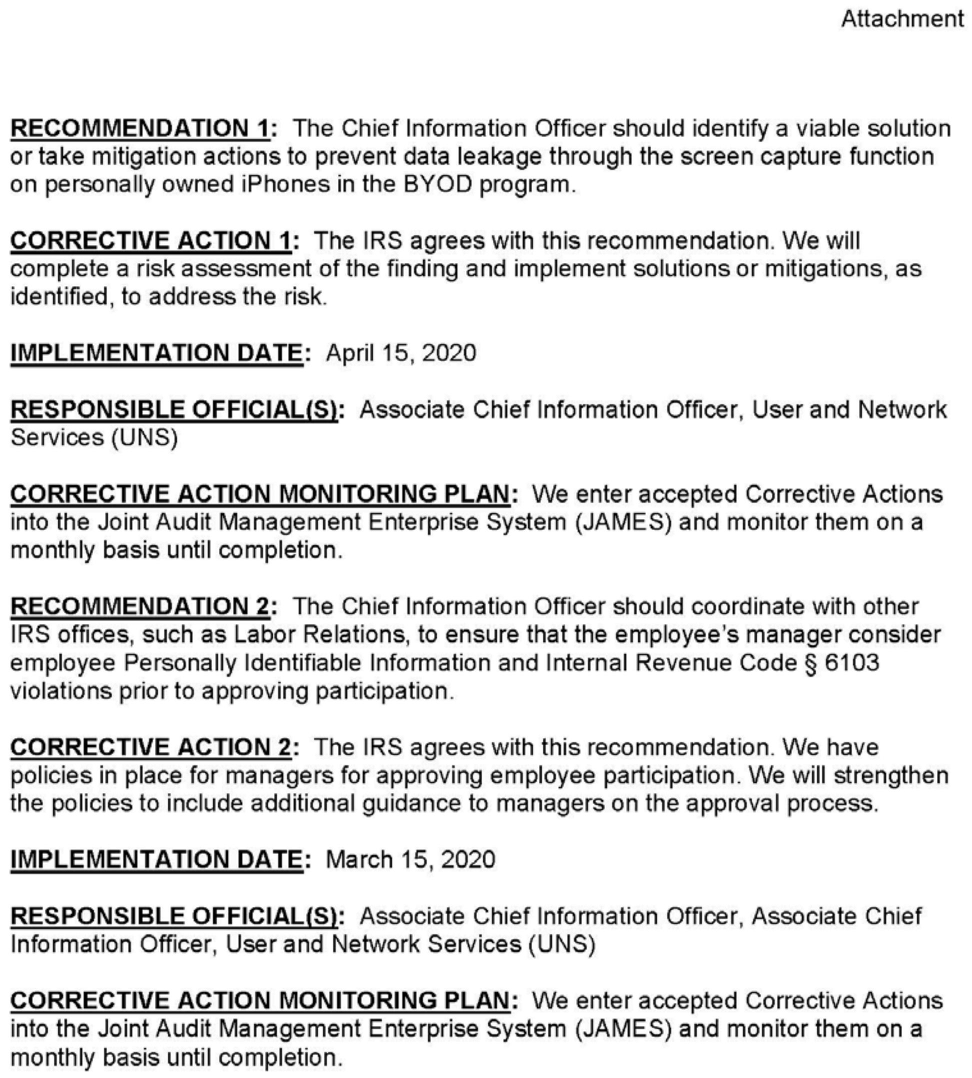


2

In closing, the IRS will continue to make improvements and address risks in these areas related to the management, technical and operational controls for the BYOD program.

The IRS values your 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 Lou Capece at (484) 636-0479.

Attachment



Attachment

RECOMMENDATION 1: The Chief Information Officer should identify a viable solution or take mitigation actions to prevent data leakage through the screen capture function on personally owned iPhones in the BYOD program.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. We will complete a risk assessment of the finding and implement solutions or mitigations, as identified, to address the risk.

IMPLEMENTATION DATE: April 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.

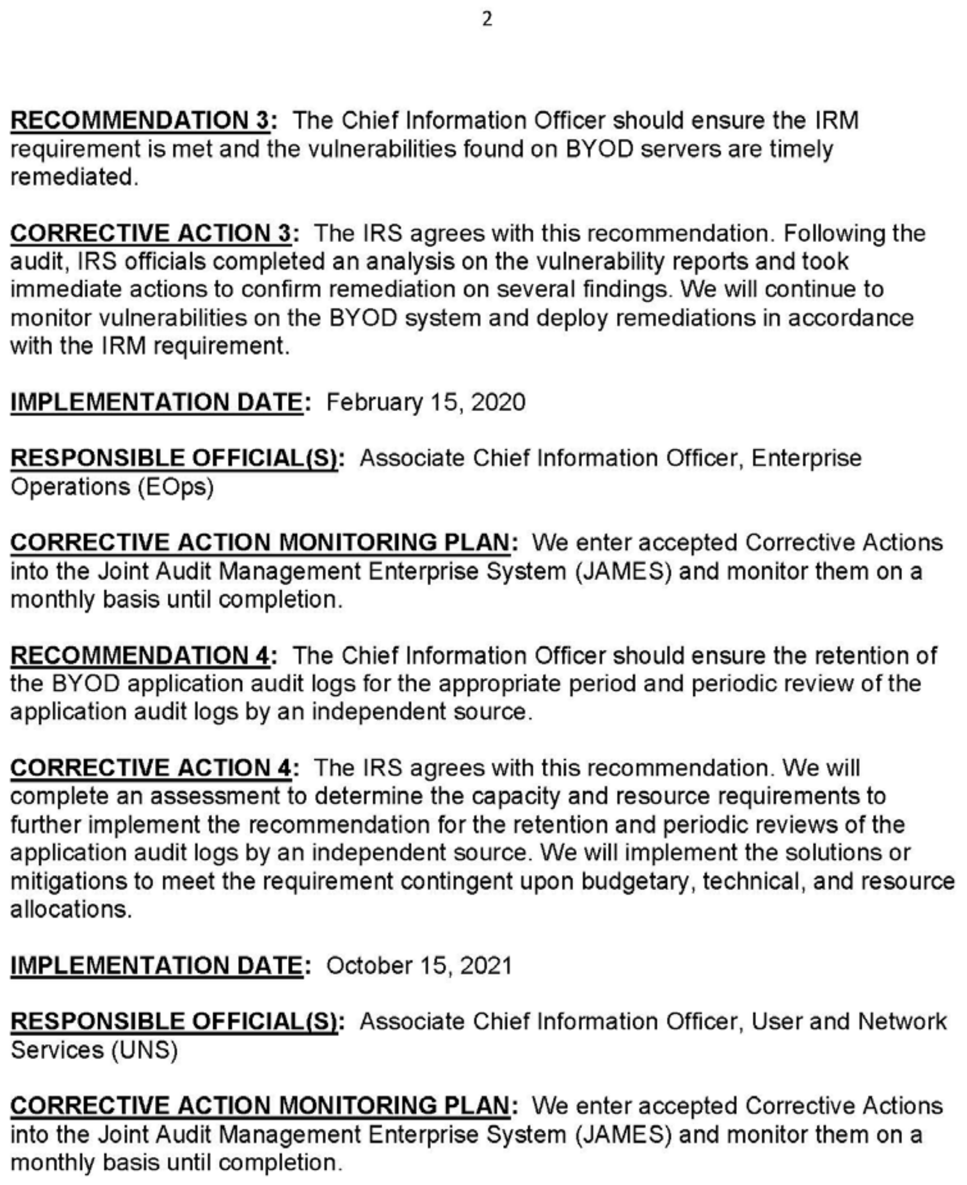
RECOMMENDATION 2: The Chief Information Officer should coordinate with other IRS offices, such as Labor Relations, to ensure that the employee's manager consider employee Personally Identifiable Information and Internal Revenue Code § 6103 violations prior to approving participation.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. We have policies in place for managers for approving employee participation. We will strengthen the policies to include additional guidance to managers on the approval process.

IMPLEMENTATION DATE: March 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, 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 3: The Chief Information Officer should ensure the IRM requirement is met and the vulnerabilities found on BYOD servers are timely remediated.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. Following the audit, IRS officials completed an analysis on the vulnerability reports and took immediate actions to confirm remediation on several findings. We will continue to monitor vulnerabilities on the BYOD system and deploy remediations in accordance with the IRM requirement.

IMPLEMENTATION DATE: February 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Operations (EOps)

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

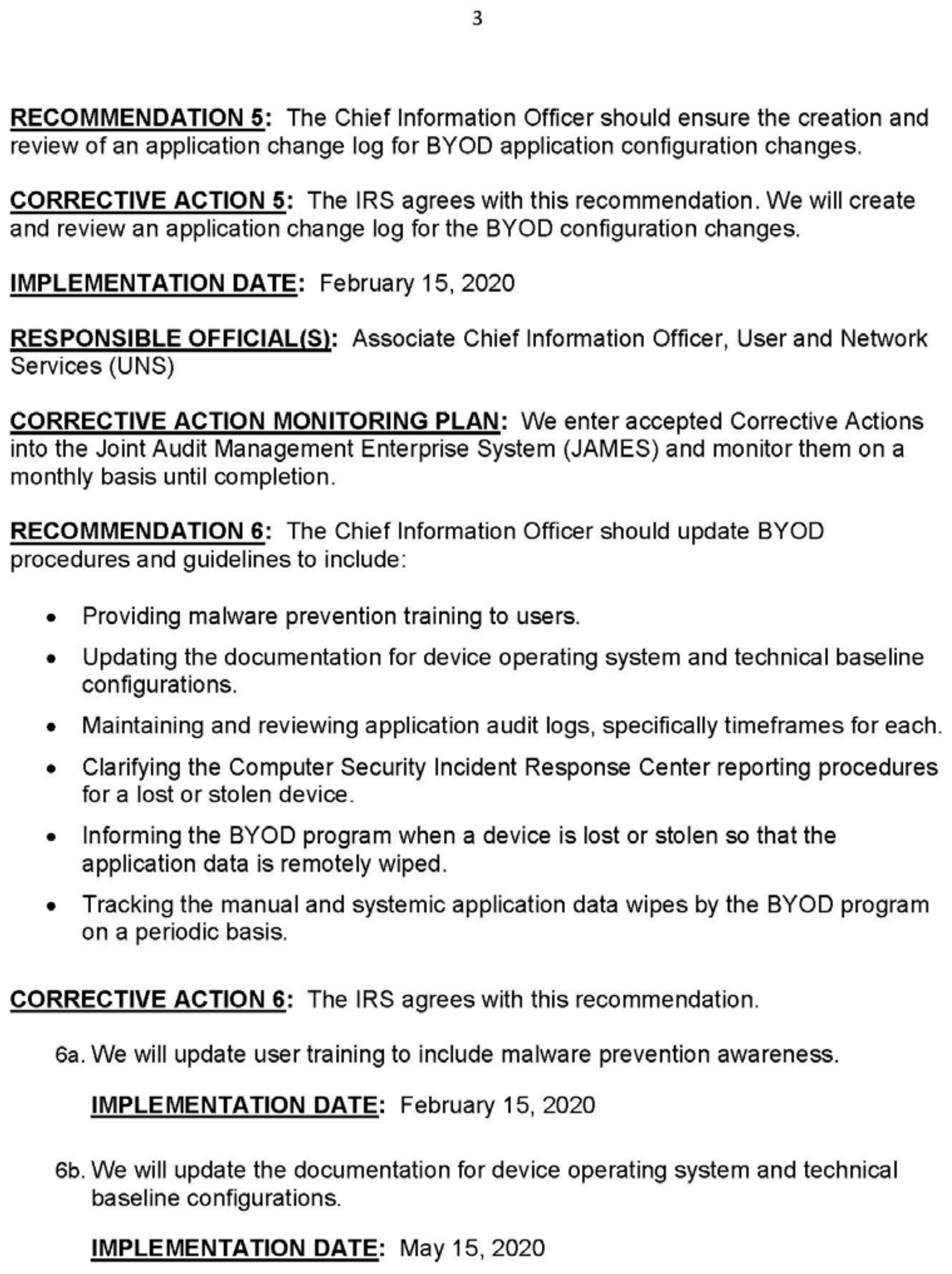
RECOMMENDATION 4: The Chief Information Officer should ensure the retention of the BYOD application audit logs for the appropriate period and periodic review of the application audit logs by an independent source.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. We will complete an assessment to determine the capacity and resource requirements to further implement the recommendation for the retention and periodic reviews of the application audit logs by an independent source. We will implement the solutions or mitigations to meet the requirement contingent upon budgetary, technical, and resource allocations.

IMPLEMENTATION DATE: October 15, 2021

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.



3

<u>RECOMMENDATION 5</u>: The Chief Information Officer should ensure the creation and review of an application change log for BYOD application configuration changes.

<u>CORRECTIVE ACTION 5</u>: The IRS agrees with this recommendation. We will create and review an application change log for the BYOD configuration changes.

<u>IMPLEMENTATION DATE</u>: February 15, 2020

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

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

<u>RECOMMENDATION 6</u>: The Chief Information Officer should update BYOD procedures and guidelines to include:

- Providing malware prevention training to users.
- Updating the documentation for device operating system and technical baseline configurations.
- Maintaining and reviewing application audit logs, specifically timeframes for each.
- Clarifying the Computer Security Incident Response Center reporting procedures for a lost or stolen device.
- Informing the BYOD program when a device is lost or stolen so that the application data is remotely wiped.
- Tracking the manual and systemic application data wipes by the BYOD program on a periodic basis.

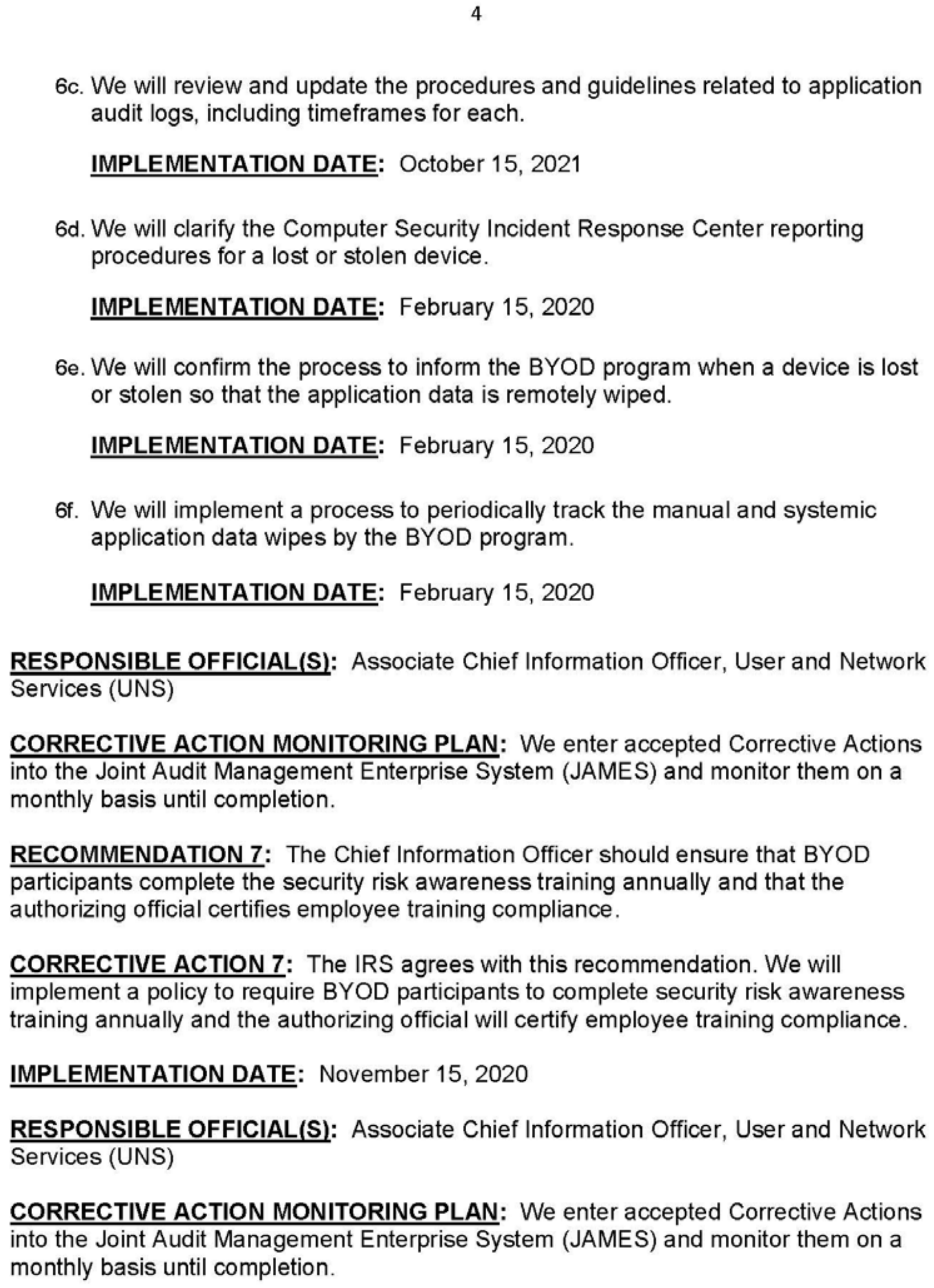
<u>CORRECTIVE ACTION 6</u>: The IRS agrees with this recommendation.

6a. We will update user training to include malware prevention awareness.

<u>IMPLEMENTATION DATE</u>: February 15, 2020

6b. We will update the documentation for device operating system and technical baseline configurations.

<u>IMPLEMENTATION DATE</u>: May 15, 2020



6c. We will review and update the procedures and guidelines related to application audit logs, including timeframes for each.

IMPLEMENTATION DATE: October 15, 2021

6d. We will clarify the Computer Security Incident Response Center reporting procedures for a lost or stolen device.

IMPLEMENTATION DATE: February 15, 2020

6e. We will confirm the process to inform the BYOD program when a device is lost or stolen so that the application data is remotely wiped.

IMPLEMENTATION DATE: February 15, 2020

6f. We will implement a process to periodically track the manual and systemic application data wipes by the BYOD program.

IMPLEMENTATION DATE: February 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 7: The Chief Information Officer should ensure that BYOD participants complete the security risk awareness training annually and that the authorizing official certifies employee training compliance.

CORRECTIVE ACTION 7: The IRS agrees with this recommendation. We will implement a policy to require BYOD participants to complete security risk awareness training annually and the authorizing official will certify employee training compliance.

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.