TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improvements Are Needed to Ensure That Wireless Networks Are Secure

September 21, 2020

Reference Number: 2020-20-063

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

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

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

To report fraud, waste, or abuse, please call us at 1-800-366-4484

HIGHLIGHTS: Improvements Are Needed to Ensure That Wireless Networks Are Secure

Final Audit Report issued on September 21, 2020
Reference Number 2020-20-063

Why TIGTA Did This Audit

Wireless access points feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network. The inherent weakness of wireless communication is that the signal is not bound by wires or walls. Because wireless communication is easily accessible, it is susceptible to attack, particularly those wireless access points in buildings with shared occupants (non-IRS organizations).

The overall objective of this review was to evaluate the effectiveness of security controls and procedures over wireless networks in use at IRS facilities and the preventative measures against unauthorized wireless access points.

Impact on Taxpayers

Wireless communications can offer many benefits, such as portability, flexibility, increased productivity, and lower installation costs. However, they can also pose significant risks to IRS critical infrastructure and assets if they are not properly implemented and secured. When wireless networks and access points are not properly secured, anyone within range of the wireless signal may gain access to the IRS network and get unauthorized access to computer resources, including systems or applications with taxpayer data, for the purpose of data theft or destruction.

What TIGTA Found

The IRS has policies and procedures that are compliant with Federal requirements and has solutions in place to monitor, scan, and maintain its wireless networks. In addition, the IRS has the ability to identify, prevent, and remove unauthorized wireless access points from its wireless networks. However, TIGTA identified areas that need improvement.

A cornerstone to developing a sound information security program is the timely identification and resolution of information security weaknesses. However, security weaknesses related to the wireless networks are not always resolved timely. The IRS is in the process of resolving 25 open security weaknesses with eight (32 percent) of the 25 weaknesses beyond the scheduled correction due date, ranging from February 2018 to April 2020. In addition, the inventory of wireless access points could be improved. TIGTA reviewed 321 wireless access points in 28 IRS locations and found 205 (64 percent) that did not have complete and accurate information on an inventory list. An inaccurate inventory hinders the IRS's ability to timely detect the loss or potential theft of the access points.

Lastly, wireless broadcast signals could be better controlled. Wireless access points are broadcasting a wireless network signal beyond IRS-controlled space, which creates the potential risk of external entities detecting and attempting to access or hack the IRS through the wireless networks. TIGTA detected the wireless signal outside of the IRS-controlled space in 21 (75 percent) of the 28 locations visited. In addition, multifunction printers are broadcasting a wireless signal, which violates IRS policy and creates a potential risk of signal interception and potential unauthorized access to the IRS's internal network.

What TIGTA Recommended

TIGTA made seven recommendations including that the Chief Information Officer resolve wireless network security-related weaknesses and ensure weakness closures are tested and approved, correct the identified wireless access point inventory issues, and require the User and Network Services function to review and better control wireless signals on its wireless access points and disable wireless signals on its multifunction printers.

The IRS agreed with six recommendations. The IRS plans to ensure that wireless security weaknesses are resolved and properly tested and closed, correct wireless access point inventory issues, update procedures to minimize wireless signal transmissions, and disable and lock wireless signals on multifunction printers. For the recommendation on improvements to its wireless inventory systems to which the IRS partially agreed, we believe the planned corrective action will address the recommendation.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 21, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Are Needed to Ensure That Wireless Networks Are Secure (Audit # 202020007)

This report presents the results of our review to evaluate the effectiveness of security controls and procedures over wireless networks in use at Internal Revenue Service (IRS) facilities and the preventative measures against unauthorized wireless access points. This review is part of our Fiscal Year 2020 Annual Audit Plan and addresses the major management and performance challenge of *Security Over 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. 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

Background

For the Internal Revenue Service (IRS), wireless communications provide many benefits, such as portability of computing resources, flexibility of using wireless versus wired connections, increased productivity to work anywhere without the need for a wired connection, and lower installation costs when setting up network connectivity in conference rooms or offices. However, wireless communications can also pose significant risks to critical infrastructure and assets if they are not properly implemented and secured. As new technologies are developed and deployed, they potentially become a major source of new vulnerabilities for which security solutions must be developed and implemented. As of December 2019, the IRS implemented Wireless Local Area Networks, hereafter referred to as wireless networks,[1] at 213 IRS locations nationwide. To access these wireless networks, the IRS installed 852 wireless access points, many of which are located in hallways, conference rooms, and training rooms. A wireless access point is a hardware device or configured node that allows wireless-capable devices to connect securely via radio transmitters and antennae to facilitate connectivity between the devices and the Internet or a network.

The inherent weakness of wireless communications is that the signal is not bound by wires or walls. Because wireless communications are easily accessible, *i.e.,* within typical signal range of 150 feet, they are susceptible to signal interception and attacks, particularly from those wireless access points in buildings with shared occupants (non-IRS organizations). Once successfully accessed, hackers would have a direct connection into the network. Wireless access points also represent potential avenues around typical external protective network measures, such as firewalls.

In addition, employees could set up a rogue access point within IRS space. This could allow non-agency (unapproved) equipment to gain access inside the IRS network by connecting through the wireless access point. This creates a higher risk situation because these connections would mimic normal network traffic and remain undetected through the rogue access point. When wireless networks and access points are not secured properly, anyone within range of the wireless signal may gain access to the network and get unauthorized access to computer resources, including systems or applications with taxpayer data, for the purpose of data theft or destruction.

The Information Technology organization's User and Network Services (UNS) function owns and operates all IRS enterprise wireless network deployments and the wireless access points. The primary core hardware infrastructure for the wireless networks is located at the Enterprise Computing Center in Memphis, Tennessee, with a backup infrastructure at the Enterprise Computing Center in Martinsburg, West Virginia. The IRS is in the process of updating several aspects of the hardware, and as a result, the wireless network infrastructure will be load balanced between both locations. In addition, the secondary core hardware for the wireless networks is located at the IRS Headquarters in Washington, D.C.

The IRS operates three distinct wireless networks, *i.e.*, internal, Bring Your Own Device, and guest, all of which operate on the same wireless access points. The internal network is for employees using IRS-issued devices (generally laptops). The Bring Your Own Device network is

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

for employees using approved personal devices or IRS-issued mobile devices. The guest network is for IRS visitors who have a bona fide temporary need.

Results of Review

The IRS has sufficient security policies and procedures over the wireless networks, and its primary guidance document, the Internal Revenue Manual (IRM), was properly aligned with the 17 selected controls for wireless network security from the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The 17 controls included *Access Control-17 Remote Access, Audit and Accountability-2 Audit Events, Physical and Environmental Protection-3 Physical Access Control,* and *System and Information Integrity-4 Information System Monitoring.* In many instances, IRM policies and procedures included additional detailed guidance related to wireless networks.

The IRS purchased two management platforms, Aruba AirWave,™ hereafter referred to as Airwave, and ClearPass,™ to monitor and manage its wireless networks. AirWave is the primary management console for the wireless networks and is the centralized place to monitor and scan for rogue devices and rogue behavior. It records all activity within the wireless networks and provides a comprehensive view of the network and potential threats and alerts if the network detects potential unauthorized access through either authentication errors or rogue devices. *2* **********2**********2**********2**********2**********2**********. A UNS function official stated that the IRS has not identified any unauthorized wireless access points connected to the network, except in one instance when an employee connected a personal hotspot to a network connection. The Network Management Control Center detected the unauthorized connection and blocked the device from communicating with the IRS network.

The ClearPass platform is used to manage user authentication, authorization, and accounting for the Bring Your Own Device and Guest wireless networks. It shows every time a user logs on to and disconnects from the wireless networks. According to UNS function officials, the IRS plans to migrate to the Cisco Identity Services Engine within the next 12 months. After the migration, ClearPass will be retired.

In addition to the positive efforts previously mentioned, we found the following areas that need improvement:

- Security weaknesses related to the wireless networks are not always resolved timely.
- The wireless access point inventory is incomplete and inaccurate.
- Wireless broadcast signals could be better controlled.

Security Weaknesses Related to the Wireless Networks Are Not Always Resolved Timely

We reviewed the Plan of Action and Milestones (POA&M) documents associated with weaknesses in the IRS's wireless networks and determined that 25 open POA&Ms were created between February 2017 and December 2019 and had scheduled completion dates between February 2018 and October 2022. Eight (32 percent) of the 25 POA&Ms were beyond the scheduled completion dates, ranging from February 2018 to April 2020. The weaknesses identified in the eight POA&Ms were as follows:

1. **********2**********
   **********2**********.
2. **********2**********.
3. User accounts are not disabled when personnel are terminated or transferred via the **********2**********.
4. **********2**********
   **********2**********.
5. **********2**********
   **********2**********
   **********2**********. A UNS function official believed that this should not be considered a weakness. **********2**********
   **********2**********
   **********2**********
   **********2**********.
6. **********2**********.
7. **********2**********
   **********2**********
   **********2**********
   **********2**********
   **********2**********
   **********2**********
   **********2**********.
8. **********2**********.

The IRS Enterprise POA&M Standard Operating Procedures version 10, dated April 2020, requires the information system owner/functional unit owner to:

- Identify and manage the development and implementation of corrective action plans for all systems they own and operate, with designated official support.
- Provide orderly, disciplined, and timely updates to the POA&M on an ongoing basis.
- Provide specific recommendations on how to correct weaknesses or deficiencies in the controls.
- Ensure that corrective actions are implemented in accordance with the Department of the Treasury standard for the POA&Ms.

- Provide monthly updates on late POA&Ms prior to the end of each month via the Treasury Federal Information Security Modernization Act (FISMA) Inventory Management System or as requested by Cybersecurity function Enterprise FISMA Services staff.[2]
- Provide updates on the POA&Ms coming due within 120 days, as requested by Cybersecurity function Enterprise FISMA Services staff.

In three of the eight POA&Ms, Cybersecurity function Enterprise FISMA Services staff recorded updates were untimely. In the remaining five, the POA&Ms have been in progress since June 2018. When we discussed the eight POA&Ms with the UNS function official responsible for the technical support for the wireless networks, he was able to provide us with evidence to support that each POA&M was being addressed. For example, one of the eight POA&Ms is a weakness related to user accounts that are not timely disabled for terminated or transferred users. This weakness is addressed by other existing policies and security measures, specifically with policies for Active Directory accounts that ensure that these types of users do not have access to the network in accordance with IRM guidance. In addition, the users' Personal Identity Verification cards, which are needed for access to the AirWave, are returned to the IRS.

For the remaining 17 POA&Ms, the UNS function official stated that nine have been addressed, but the POA&Ms have not been closed. The evidence that supports the POA&Ms' closures has been provided to the appropriate UNS function personnel for uploading to the Treasury FISMA Inventory Management System for subsequent testing and closure approval. Because this information was provided to us as we completed our audit, we did not evaluate the evidence to determine whether the proposed closure actions would effectively address the security weakness. For the remaining eight POA&Ms, the IRS is still working to resolve the weaknesses by requesting evidence and clarification from other UNS offices.

A cornerstone to developing a sound information security program is the timely identification and resolution of information security weaknesses. Failure to resolve existing wireless network security weaknesses in accordance with IRM and NIST requirements compromises the security posture of the system. This could lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing and exploitation, which all compromise the integrity, confidentiality, and availability of the system.

Recommendation 1: The Chief Information Officer should ensure that the 25 wireless network security-related weaknesses are resolved and that the evidence supporting the weakness closures is updated in the Treasury FISMA Inventory Management System for subsequent testing and closure approval.

Management's Response: The IRS agreed with this recommendation. The IRS will ensure that the 25 wireless network security-related weaknesses are resolved and updated in the Treasury FISMA Inventory Management System with supporting closure evidence for testing and closure approval.

[2] This function has program oversight for all POA&M items across the IRS.

The Wireless Access Point Inventory Is Incomplete and Inaccurate

As stated earlier, the IRS installed 852 wireless access points nationwide. We visited 28 IRS locations in four metropolitan regions across the United States **********2********** **********2********** and selected a judgmental sample of 321 (38 percent) of the 852 wireless access points to perform a physical verification of the access points.[3] In total, we found inventory errors on 205 (64 percent) of the 321 wireless access points reviewed.

We were unable to locate 27 (13 percent) of the 205 wireless access points with inventory errors. When we shared our results with the IRS, a UNS function official stated that 15 devices were stored elsewhere in the same location or moved to another off-site location, one device was sent to a site for testing, and four devices were returned to a deployment team for reallocation. Because this information was provided to us as we completed our audit, we were unable to physically verify the updated status for the 20 devices. The remaining seven devices could not be accounted for.

For the remaining 178 wireless access points, the inventory information had not been updated to properly reflect the location of the access points, and access points were not correctly labeled.[4] Specifically, we found the following issues:

- 166 devices were either missing the IRS-assigned access point name or the name was different than what was shown on the inventory list.
- 27 devices were found in a location, *i.e.,* a room, that was different than what was shown on the inventory list.
- 4 devices had an IRS inventory barcode that was different from what was shown on the inventory list.

In addition, we found 13 wireless access points that were installed but were not included in the inventory list that we used during our visits. In March 2020, a UNS function official provided an updated inventory list, and we were able to account for eight of the 13 devices. The remaining five devices were not on the inventory list even though they were installed as official wireless access points.

NIST Special Publication 800-53 Revision 4 requires that organizations develop and document an inventory of information system components that 1) accurately reflect the current information systems, 2) include all components within the authorization boundary of the information system, 3) is at the level of granularity deemed necessary for tracking and reporting, and 4) include information deemed necessary to achieve effective information system component accountability. In addition, organizations should review and update the information system component inventory.[5]

IRM 10.8.1.4.11.2, *Physical and Environmental Protection-3 Physical Access Control* (May 9, 2019), requires the IRS to inventory physical access devices at a minimum annually. A

[3] See Appendix I for the detailed methodology for selecting the judgmental sample. A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[4] The total number of exceptions will not equal 178 because some wireless access points had multiple inventory issues.
[5] IRM 10.8.1.4.5.7 (1), (2), *Configuration Management-8 Information System Component Inventory* (July 8, 2015), supports the NIST criteria.

UNS function official stated that the standard operating procedures do not provide the specific inventory steps to deploy, move, replace, or retire wireless devices. In addition, the procedures do not include taking photographs of the devices including the barcode and device name and verification that the name and location match the inventory list.

When we asked about the last inventory review conducted, a UNS function official explained that the IRS started an enterprise-wide asset management validation process in May 2019. The asset management deployment team closely tracked the inventory on a spreadsheet and in the Hewlett Packard Asset Manager tool, and this work was still in process when we started the audit. Specifically, the asset management team started a validation of assets to determine whether the value and information were correct. The UNS function Network Management Control Center also assembled a team to validate all assets it managed, including wireless access point devices. The UNS function began the last inventory validation during the summer of 2019 and submitted the validations and updates to asset management officials on March 4, 2020. The UNS function was in the middle of the validation process when we requested the December 2019 inventory list.

According to UNS function officials, the IRS manages the wireless access point inventory through a combination of the Hewlett Packard Asset Manager tool and the AirWave management platform. The system and platform do not communicate and share data. As such, changes to the wireless access points that are recorded in the AirWave as part of day-to-day management of the wireless networks are not automatically reflected in the IRS's official asset management system. The local network teams are responsible for maintaining the network at their location, *e.g.,* deployment and replacement. According to a UNS function official, network teams would move the devices to different locations within the same site location or to another new location without making all parties aware of the changes. We identified an example of this occurrence during the audit. During our discussions with UNS function personnel, we determined that a wireless access point had been reported offline and not functioning. When the IRS attempted to locate the device, it could not be found and was subsequently reported as missing. When we performed our physical verification, we were able to identify the device and share its location with the UNS function.

Having an incomplete or inaccurate inventory, including the inaccurate locations or names of wireless access points, can impede IRS management's ability to manage the assets within the wireless networks or locate and troubleshoot any technical issues that may occur. In addition, an inaccurate inventory hinders the IRS's ability to timely detect the loss or potential theft of the access points.

The Chief Information Officer should:

Recommendation 2: Correct the wireless access point inventory issues that we identified and shared with management.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will correct the wireless access point inventory issues identified during the audit, contingent on resource and funding availability.

Recommendation 3: Update the internal procedures to provide detailed requirements for reviews and updates to the wireless access point inventory, including taking photographs of the devices during the deployment and replacement stages.

Management's Response: The IRS agreed with this recommendation. The IRS will update internal procedures for access point deployment and replacement and inventory management, including guidance for taking photographs typical of wireless access point deployments.

Recommendation 4: Improve the current inventory management system and platform to ensure that all changes to wireless access point components are updated simultaneously.

Management's Response: The IRS partially agreed with this recommendation. The IRS agreed that the efficiency and accuracy of wireless access point inventory can be improved. However, it disagreed with the recommendation to ensure that all changes are updated simultaneously in the current inventory management system and platform. The IRS will complete an assessment to determine the appropriate method for maintaining accurate and timely updates to the current inventory management system and platform and implement a process to address the recommendation.

Office of Audit Comment: While the IRS partially agreed, we believe its planned corrective action will address this recommendation.

Wireless Broadcast Signals Could Be Better Controlled

While conducting our inventory verification, we also tested the wireless access point broadcast signal strength and determined that the wireless signals extended well beyond the IRS-controlled space in 21 (75 percent) of the 28 locations visited. For example, in one location, we detected the wireless signal from one wireless access point in a loading dock several floors away from the IRS space. In other locations, we detected the wireless signal in public parking lots, outside the front door of the building that housed an IRS office, and outside of a building with an IRS office facing the street. We did not identify any signal boosting or enhanced wireless signal devices at any of the locations we visited. Figure 1 is a summary of the locations we found with wireless signals that extended beyond IRS-controlled spaces.

Figure 1: Summary of Locations With Wireless Access Point Ranges That Extended Beyond IRS-Controlled Spaces

Metropolitan Regions	Number of Locations	Number of Locations With Extended Signal	Percentage
*****2*****	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**
Total	**28**	**21**	**75%**

Source: Treasury Inspector General for Tax Administration analysis of scanned wireless access points in IRS offices.

IRM 10.8.55.3.8.1, *Risk Assessment-3 Risk Assessment* (July 5, 2019), requires that wireless access point range boundaries be tested to measure and establish the precise extent of the wireless

coverage. IRM 10.8.1.4.1.17.1, *Access Control-18 Wireless Access – Control Enhancements* (July 8, 2015), requires the IRS to select radio antennas and calibrate transmission power levels to reduce the probability that usable signals can be received outside of IRS-controlled boundaries, such as facilities, property, and offices. IRM 10.8.1 guidance comes directly from NIST Special Publication 800-53, Revision 4. The publication elaborates by stating that actions may be taken by organizations to limit unauthorized use of wireless communications outside of the organization-controlled boundaries to include "reducing the power of the wireless transmissions, employing measures to control wireless emanations, and using directional/beam forming antennas."

When we asked the IRS what evaluations were performed regarding the ranges of the access points, UNS function officials stated that, when the IRS initially deployed the wireless networks, it did not reduce the access point signal strength. However, when the IRS updated its guidance in Calendar Year 2015, it required the power levels be adjusted to reduce the signal range, and in Calendar Year 2019, it required the range boundaries to be tested and measured. A UNS function official stated that the IRS is in the process of reducing the access point signal strength in an effort to limit the range. In addition, the IRS is preparing to replace a significant number of the access points with a newer model. As a part of this equipment refresh, the UNS function plans to upload existing floor plans in a location and mapping feature in the AirWave to help determine the best access point locations. The UNS function official also provided, as an example, planning and design documents for two locations that included a heat coverage map with a color-coded legend to describe the intended coverage area and the strength of the signal from the strongest to the weakest but that still would allow the user to access the wireless networks and perform work.

While the IRS has the ClearPass platform in place for controlling access to the Bring Your Own Device and guest wireless networks to mitigate some of this risk, no system is completely secure. By having the wireless network signal broadcasting beyond its controlled space, the IRS is increasing the risk that hackers might be able to intercept the wireless broadcast signal and hack their way into the IRS network via the signal. While wireless signals cannot be completely contained due to the inherent nature of the signal, reducing the signal strength as much as possible will minimize the risk to the IRS's internal network.

Multifunction printers are broadcasting a wireless signal, which violates policy and creates unnecessary risk

While testing wireless access point broadcast signal strength, we detected 90 printers broadcasting a wireless signal in the 28 locations we visited. These printers are not directly managed and secured by the wireless network team, but we believe they pose a security risk and should be addressed. Because the IRS was not the only occupant in many of the buildings and our scans captured limited information, *i.e.,* the name of the printer that was broadcasting and the wireless network address for each device, we were unable to determine if all of the multifunction printers identified belonged to the IRS. We provided the scan data to the IRS, but the IRS was unable to confirm whether the multifunction printers were IRS-owned because it did not maintain a record of the wireless network address for multifunction printer devices. However, we were able to conclude that 24 of the 90 multifunction printers were detected in locations where only IRS personnel resided. A UNS function official acknowledged that there are IRS printers broadcasting a wireless signal. While the wireless networks do not control the wireless signals broadcasting from the multifunction printers, the devices had wireless capability

and were broadcasting a wireless signal. As a result, the multifunction printers were noncompliant with IRM policies.

IRM 10.8.1.4.1.17, *Access Control-18 Wireless Access* (July 8, 2015), requires the IRS to ensure that unapproved wireless networking capabilities of desktops, laptops, printers, copiers, fax machines, and other devices shall be disabled through automated means (where technically possible) and monitored through automated means for unauthorized changes.
IRM 10.8.1.4.16.6.3.3, *Printers* (May 9, 2019), states that the wireless capability shall be disabled on a printer.

When discussing this issue with the IRS, UNS function officials thought that the multifunction printers in question might be primarily desktop types that do not have IRS network connections but are connected to the laptops through a universal serial bus cable. We agree that a multifunction printer broadcasting a wireless signal that is not connected to the network is a lower risk. However, we believe multifunction printers with wireless signals that are connected to an employee's computer are still an unnecessary risk, which creates potential for a bad actor to attempt to find their way into the IRS network through the multifunction printer.

When we asked why the wireless capabilities of the multifunction printers were not disabled prior to issuance and installation, UNS function personnel responded that the printers are not configured prior to being shipped to employees. However, UNS function officials indicated that they plan to: 1) work with telecommunications personnel to identify where the printers with wireless signals are located, 2) run the setup command and turn off the wireless feature, and 3) come up with a standard to install non-network printers. However, they did not provide a timeline for completing these tasks. While the plans are a good first step, they did not contain sufficient details about 1) the standards and whether they will include details about how monitoring for wireless capability will occur, 2) whether the wireless on/off switch would be locked to ensure that it would not be enabled again, and 3) whether the plans will include actions to be taken when multifunction printers are replaced.

To be compliant with IRM requirements and to mitigate the potential risk of a hacker intercepting a wireless signal and attempting to access the IRS network, the IRS should disable and lock the wireless capability to prevent wireless broadcasting on all IRS printers.

The Chief Information Officer should ensure that:

Recommendation 5: The UNS function reviews and minimizes the broadcast range of the wireless access point signals to be within IRS-controlled boundaries. In addition, ensure that the broadcast range for the wireless access points planned for model replacement is minimized.

Management's Response: The IRS agreed with the recommendation. The IRS will update procedures to minimize transmission of wireless access point signals outside IRS-controlled boundaries, as appropriate, while continuing to mitigate any security risks.

Office of Audit Comment: While the IRS agreed with this recommendation, the IRS's planned corrective action only stated that it will update procedures to minimize transmission of wireless access point signals. As long as the updated procedures are effectively implemented, we believe the planned corrective action will address this recommendation.

Recommendation 6: The UNS function disables and locks the wireless capability in multifunction printers to comply with IRM policy.

Management's Response: The IRS agreed with the recommendation. The IRS will complete an assessment to determine the appropriate method for addressing this recommendation and to update the multifunction printers identified during the audit to disable and lock the wireless capability in accordance with IRM policy.

Office of Audit Comment: While the IRS agreed with this recommendation, the IRS's planned corrective action to disable and lock the wireless capability on the multifunction printers appears to only apply to those multifunctional printers identified during the audit. Our recommendation is directed at all IRS multifunction printers to ensure compliance with its internal policy.

Recommendation 7: UNS function multifunction printer action plans include details that will address multifunction printer monitoring and disabling and locking the wireless signal capability.

Management's Response: The IRS agreed with the recommendation. The IRS will update the action plans for multifunction printers to include detailed requirements to address the monitoring and disabling of the wireless signal capability.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the effectiveness of security controls and procedures over wireless networks in use at IRS facilities and the preventative measures against unauthorized wireless access points. To accomplish our objective, we:

- Evaluated whether the IRS's policies and procedures complied with 17 selected controls for wireless network security from the NIST Special Publication 800-53 Revision 4 requirements.
- Selected a judgmental sample[1] of the IRS offices and associated wireless access points to physically inspect and verify. We used this sampling method to allow for the varied conditions, *i.e.,* a sufficient sample size to most represent the population of wireless access points to form a reasonable basis for conclusions, without projecting. We selected multiple offices in central locations across the Nation with a varied quantity of wireless access points from large to small. The IRS provided the December 2019 inventory of wireless access points for 213 locations with 852 wireless access points for our review. **********2********** **********2**********. We selected additional locations in the ********2********** with a varied quantity of wireless access points. Next, we wanted to be geographically dispersed across the Nation, so we selected additional metropolitan regions for a total sample of 321 access points from 28 locations. ******2********** **********2**********. We photographed each wireless access point, when possible, to identify the barcode and the name on the device. We compared this information with the inventory list for accuracy and completeness.
- Performed scans of the wireless environment at each site reviewed and engaged an Applied Research and Technology data analyst to analyze the scan results for multifunction printers broadcasting wireless signals and the range of the IRS's wireless signals.
- Inspected each site for any signal boosting or other equipment to enhance wireless signals for the IRS's distinct wireless networks.
- Obtained and reviewed the POA&M documents associated with the 25 open security weaknesses in the IRS's wireless networks from the IRS and the Treasury FISMA Inventory Management System.
- Evaluated the IRS's mechanisms to monitor and secure the wireless networks by observing, reviewing procedures, and interviewing UNS function personnel regarding the Airwave and ClearPass platforms used to monitor and manage the wireless networks.

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

Performance of This Review

This review was performed at the **********2********** ********** during the period October 2019 through July 2020. 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; Michael Segall, Lead Auditor; Suzanne Westcott, Senior Auditor; and Lance Welling, Information Technology Specialist (Data Analytics).

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 wireless access points. We evaluated the data by 1) reviewing the inventory list provided for completeness and 2) selecting a sample of access points to test for accuracy and completeness as part of our audit procedures. We determined that the data were sufficiently reliable to conduct our detailed testing of the IRS's inventory for the purposes of this report.

We performed minimal tests to assess the reliability of the data from the scanning software. We evaluated the data by 1) obtaining data from the scanning software used at each of the IRS locations, 2) combining the scanning data into usable spreadsheets, and 3) reviewing the files to ensure that they were complete based on the original scan files. 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: IRS policies and procedures and NIST Special Publication 800-53 Revision 4 requirements for monitoring and controlling access to the wireless network, procedures for managing the inventory of the wireless access points, and policies and procedures for issuing printers to IRS employees. We evaluated these controls by reviewing the criteria applicable to the wireless networks and use of multifunction printers at the IRS, assessing the IRS's wireless access point inventory, interviewing UNS function personnel, and reviewing and analyzing documentation related to the monitoring of the wireless networks.

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; 205 wireless access points with incomplete and inaccurate inventory information (see Recommendation 2).

Methodology Used to Measure the Reported Benefit:

We selected a judgmental sample[1] of IRS locations and associated wireless access points to physically inspect and verify across the Nation with a varied quantity of wireless access points from large to small. The IRS provided the December 2019 inventory of wireless access points for 213 IRS locations with 852 wireless access points for our review. We sampled 321 access points from 28 locations in four metropolitan regions – **********2********** **********2**********. In total, we found inventory errors on 205 (64 percent) of the 321 wireless access points reviewed.

We were unable to locate 27 devices for various reasons. A UNS function official stated that 15 devices were stored elsewhere in the same location or moved to another off-site location, one device was sent to a site for testing, and four devices were returned to a deployment team for reallocation. While we were unable to verify the status of the 20 devices, the remaining seven devices could not be accounted for.

For the remaining 178 devices,[2] the inventory information had not been updated to properly reflect the location of the access points, and access points were not correctly labeled. Specifically, we found the following issues:

- 166 devices were either missing the access point name the IRS assigned or the name was different than what was shown on the inventory list.
- 27 devices were found in a location, *i.e.,* a room, that was different than what was shown on the inventory list.
- 4 devices had an IRS inventory barcode that was different from what was shown on the inventory list.

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[2] The total number of exceptions will not equal 178 because some wireless access points had multiple inventory issues.

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 24 IRS multifunction printers that are unnecessarily broadcasting a wireless signal (see Recommendation 6).

Methodology Used to Measure the Reported Benefit:

We performed scans of the wireless environment at each of the 28 locations reviewed. Those scans listed multifunction printers that were broadcasting a wireless signal. Throughout the 28 locations, the scans recorded 90 printers that could potentially be IRS printers broadcasting a wireless signal in violation of the IRM. Based on the information we provided, *i.e.,* the name of the multifunction printer that was broadcasting and the wireless network address for each device, the IRS was unable to confirm whether the multifunction printers were IRS-owned. We reviewed the scan results and concluded that, because the multifunction printers were detected in locations where there were only IRS offices, 24 of the 90 multifunction printers could potentially belong to the IRS.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 15, 2020

MEMORANDUM FOR MICHAEL E. MCKENNEY,
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger Nancy A. Sieger Digitally signed by Nancy A. Sieger Date: 2020.09.14 16:26:14-04'00'
Acting Chief Information Officer

SUBJECT: Draft Audit Report – Improvements Are Needed to Ensure That Wireless Networks Are Secure (Audit # 202020007) (e-trak # 2020-25953)

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss their observations. The Internal Revenue Service (IRS) is committed to continually improving its wireless network security and services, including the reliability of our wireless asset inventory. We appreciate TIGTA's recognition of the IRS's progress and continual improvement in these areas. As noted in the report, the IRS security policies and procedures are properly aligned with the 17 National Institute of Standards and Technology (NIST) selected controls for wireless network security.

We also appreciate TIGTA's acknowledgement that the IRS provided evidence of mitigating identified risks. To further strengthen security for devices connecting wirelessly, certificate-based machine authentication was implemented to complement the existing certificate-based user authentication and role-based access control. This enhancement improves security for network resources and taxpayer data, ensuring only authorized wireless devices are allowed access to the IRS internal network.

The IRS recognizes the importance of timely identification and resolution of information security weaknesses and maintaining complete and accurate inventory. During the audit fieldwork, we also took immediate action to identify necessary procedural changes and began validating new deployment guidelines. We continue to validate and improve the accuracy of our inventory data and believe these actions reflect our commitment to continually strengthening system security and addressing TIGTA's recommendations.

Attached is our detailed corrective action plan to address the audit report's recommendations. The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 317-5000 or Frank Kist at (240) 613-4041.

Attachment

Attachment

Draft Audit Report – Improvements Are Needed to Ensure
That Wireless Networks Are Secure (Audit # 202020007) (E-trak # 2020-25953)

RECOMMENDATION 1: The Chief Information Officer should ensure that the 25 wireless network security-related weaknesses are resolved and that the evidence supporting the weakness closures is updated in the Treasury FISMA Inventory Management System for subsequent testing and closure approval.

CORRECTIVE ACTION: The IRS agrees with the recommendation. We will ensure that the 25 wireless network security-related weaknesses are resolved and updated in the Treasury Inventory Management System with supporting closure evidence for testing and closure approval.

IMPLEMENTATION DATE: December 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.

RECOMMENDATION 2: Correct the wireless access point inventory issues that we identified and shared with management.

CORRECTIVE ACTION: The IRS agrees with the recommendation. We will correct the wireless access point inventory issues identified during the audit contingent upon resource and funding availability.

IMPLEMENTATION DATE: December 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.

Attachment

Draft Audit Report – Improvements Are Needed to Ensure
That Wireless Networks Are Secure (Audit # 202020007) (E-trak # 2020-25953)

RECOMMENDATION 3: Update the internal procedures to provide detailed requirements for reviews and updates to the wireless access point inventory, including taking photographs of the devices during the deployment and replacement stages.

CORRECTIVE ACTION: The IRS agrees with the recommendation. We will update internal procedures for access point deployment and replacement and inventory management, including guidance for taking photographs typical of wireless access point deployments.

IMPLEMENTATION DATE: June 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.

RECOMMENDATION 4: Improve the current inventory management system and platform to ensure that all changes to wireless access point components are updated simultaneously.

CORRECTIVE ACTION: The IRS partially agrees with the recommendation. We agree that the efficiency and accuracy of wireless access point inventory can be improved. However, we disagree with the recommendation to ensure all changes are updated simultaneously in the current inventory management system and platform. The IRS will complete an assessment to determine the appropriate method for maintaining accurate and timely updates to the current inventory management system and platform and implement a process to address the recommendation.

IMPLEMENTATION DATE: November 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.

Attachment

Draft Audit Report – Improvements Are Needed to Ensure
That Wireless Networks Are Secure (Audit # 202020007) (E-trak # 2020-25953)

RECOMMENDATION 5: The UNS function reviews and minimizes the broadcast range of the wireless access point signals to be within IRS-controlled boundaries. In addition, ensure that the broadcast range for the wireless access points planned for model replacement is minimized.

CORRECTIVE ACTION: The IRS agrees with the recommendation. We will update procedures to minimize transmission of wireless access point signals outside IRS-controlled boundaries, as appropriate, while continuing to mitigate any security risks.

IMPLEMENTATION DATE: September 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.

RECOMMENDATION 6: The UNS function disables and locks the wireless capability in multifunction printers to comply with IRM policy.

CORRECTIVE ACTION: The IRS agrees with the recommendation. We will complete an assessment to determine the appropriate method for addressing this recommendation and to update the multifunction printers identified during the audit to disable and lock the wireless capability in accordance with Internal Revenue Manual (IRM) policy.

IMPLEMENTATION DATE: December 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.

Attachment

Draft Audit Report – Improvements Are Needed to Ensure
That Wireless Networks Are Secure (Audit # 202020007) (E-trak # 2020-25953)

RECOMMENDATION 7: UNS function multifunction printer action plans include details that will address multifunction printer monitoring and disabling, and locking the wireless signal capability.

CORRECTIVE ACTION: The IRS agrees with the recommendation. While we continue to effectively mitigate any security risks, we will update the action plans for multifunction printers to include detailed requirements to address the monitoring and disabling of the wireless signal capability.

IMPLEMENTATION DATE: June 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.

Attachment II

Draft Audit Report – Improvements Are Needed to Ensure
That Wireless Networks Are Secure (Audit # 202020007) (E-trak # 2020-25953)

Type and Value of Outcome Measure:
Reliability of Information – Potential; 205 wireless access points with incomplete and inaccurate inventory information (see Recommendation 2).

We agree and during the audit IRS officials took immediate action to evaluate and update current processes and procedures that will further improve the reliability of information for wireless access point inventory data.

Type and Value of Outcome Measure:
Taxpayer Privacy and Security – Potential; 24 IRS multifunction printers that are unnecessarily broadcasting a wireless signal (see Recommendation 6).

We agree and have already begun an effort to develop a solution to address the remediation and potential risk associated with multifunction printers.

Nancy A. Sieger Digitally signed by Nancy A. Sieger Date: 2020.09.14 16:27:15 -04'00'

Nancy A. Sieger
Acting Chief Information Officer

Appendix IV

Glossary of Terms

Term	Definition
Access Control-17 Remote Access	A NIST security control in which an organization establishes and documents the usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. In addition, the organization authorizes remote access to the information system prior to allowing such connection.
Active Directory	A Microsoft® Windows domain service that blends authentication, authorization, and directory technologies to create enterprise security boundaries that are highly scalable. Active Directory also enables administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization simultaneously from a central, organized, accessible database.
AirWave	A scalable, full-featured management solution for multivendor wired and wireless networks that integrates configuration and deployment and real-time visibility and control for comprehensive management and troubleshooting. AirWave provides a flexible platform to maintain the reliability and performance of Aruba access points, controllers, switches, and multivendor devices.
Aruba	A Hewlett Packard enterprise company that provides networking solutions such as delivering secure and reliable wireless to mobile users. The IRS is using Aruba solutions for its network environment.
Audit and Accountability-2 Audit Events	A NIST security control in which an organization establishes that the information system is capable of auditing organization-defined auditable events. An example of this control is that wireless access point logging shall be enabled.
Cisco Identity Services Engine	A software product identified as the solution to manage wired, wireless, and virtual private network access connections to the internal network. In addition, it is a security management platform that provides user and device authentication.
ClearPass	A policy management platform that provides role and device-based secure network access control for Bring Your Own Device and corporate devices as well as employees, contractors, and guests across wired, wireless, and virtual private network infrastructures.
Controller	A hardware device or a software program that manages or directs the flow of data between two entities. A controller can be thought of as something that interfaces between two systems and manages communications between them.

Term	Definition
Firewall	Software used to maintain the security of the IRS's network by blocking unauthorized network traffic to or from IRS systems. It is employed to prevent unauthorized web users or illicit software from gaining access to the network that is connected to the Internet. It is the first line of defense to secure sensitive information. The IRS has installed firewalls at its connections with the Internet, its business partners, and its internal network.
Hewlett Packard Asset Manager	A tool that is used by the IRS to track asset management activities for the full life cycle of hardware information technology and non–information technology investigative equipment from acquisition to disposal. It is also referred to as the Knowledge, Incident/Problem, Service Asset Management – Asset Manager module.
Load Balanced	A process that helps make networks more efficient. It distributes the processing and traffic evenly across a network, making sure no single device is overwhelmed.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal Government agency operations and assets.
Node	Any system or device connected to a network. For example, if a network connects a file server, five computers, and two printers, there are eight nodes on the network.
Physical and Environmental Protection-3 Physical Access Control	A NIST security control for which an organization inventories its defined physical access devices for a defined frequency.
Rogue Access Point	Any wireless access point that has been installed on a network's wired infrastructure without the consent of the network's administrator or owner, thereby providing unauthorized wireless access to the network's wired infrastructure.
System and Information Integrity-4 Information System Monitoring	A NIST security control for which an organization 1) monitors information systems to detect attacks and indicators of potential attacks; 2) identifies unauthorized use of the information system through the organization's defined techniques and methods; 3) deploys monitoring devices; and 4) protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
Universal Serial Bus	The most popular connection used to connect a computer to devices such as digital cameras, printers, scanners, and external hard drives.
Wireless Local Area Network	A wireless distribution method for two or more devices that uses high-frequency radio waves and often includes an access point to the Internet.

Appendix V

Abbreviations

FISMA	Federal Information Security Modernization Act of 2014
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
UNS	User and Network Services