TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Active Directory Oversight Needs Improvement

February 5, 2020

Reference Number: 2020-20-006

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

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

ACTIVE DIRECTORY OVERSIGHT NEEDS IMPROVEMENT

Highlights

Final Report issued on February 5, 2020.

Highlights of Reference Number: 2020-20-006 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

Microsoft® Active Directory is a Windows domain service that blends authentication, authorization, and directory technologies to create enterprise security boundaries that are highly scalable. Security weaknesses in the Active Directory could allow unauthorized access to critical IRS servers, applications, and account management. Without adequately protecting Active Directory domain controllers, the IRS cannot ensure that sensitive taxpayer information is protected.

WHY TIGTA DID THE AUDIT

This audit was initiated to review the Active Directory Technical Advisory Board's effectiveness in implementing our previous recommendations and to evaluate the effectiveness and efficiency of the Integrated Submission and Remittance Processing (ISRP) Active Directory implementation.

WHAT TIGTA FOUND

TIGTA previously recommended that the IRS review the scope of the Active Directory Technical Advisory Board's defined oversight responsibilities and update the existing charter to ensure that all individual forest owners are appropriately represented on the Active Directory Technical Advisory Board. The IRS implemented our previous recommendations.

TIGTA's review of the ISRP's implementation of the Active Directory found that computer rooms containing ISRP domain controllers lacked physical security and environmental controls. TIGTA identified 15 physical security violations related to Limited Areas, multifactor authentication, fire safety and suppression, and emergency power shutoff.

The ISRP Active Directory architecture lacks necessary logical security controls. For example, the IRS did not previously use credentials while performing vulnerability scans on ISRP domain controllers. When the IRS performed vulnerability scans using credentials at our request, the scans reported a 312 percent increase in the vulnerabilities identified. The IRS is also using an outdated application to perform security compliance checks.

Further, the IRS improperly configured ISRP service and business role accounts. As a result, TIGTA found more than 16,000 policy violations. Finally, the IRS inappropriately assigned business role accounts to an administrator group, resulting in those accounts having unnecessary elevated privileges.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer should ensure that computer rooms are immediately updated to comply with agency and Federal requirements; physically separate the submission processing equipment from the ISRP domain controllers; prioritize computer room upgrades to ensure access via multifactor authentication; establish a process to review monthly vulnerability scan reports for credentialed scans; ensure that credentialed scans are regularly completed; ensure that ISRP domain controllers with critical and high vulnerabilities are properly remediated; ensure that compliance checker applications use up-to-date guidelines; ensure that all ISRP business role accounts and service accounts are in compliance with agency requirements; and ensure that system administrators have only one privileged account with domain administrator privileges.

The IRS agreed with all of our recommendations. The IRS plans to update computer rooms housing ISRP domain controllers to comply with physical security requirements; review vulnerability scans and verify credentialed vulnerability scans are conducted; remediate critical and high vulnerabilities; monitor device configurations; properly configure business role accounts; and review administrator groups and remove duplicate accounts.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

February 5, 2020

MEMORANDUM FOR COMMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Active Directory Oversight Needs Improvement (Audit # 201920013)

This report presents the results of our review of the Active Directory Technical Advisory Board's effectiveness in implementing our previous recommendations and the effectiveness and efficiency of the Integrated Submission and Remittance Processing Active[1] Directory implementation. This audit is included in our Fiscal Year 2020 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 VI.

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).

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

Table of Contents

Abbreviations

AD	Active Directory
ADTAB	Active Directory Technical Advisory Board
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISRP	Integrated Submission and Remittance Processing
NIST	National Institute of Standards and Technology
PIV	Personal Identity Verification
TIGTA	Treasury Inspector General for Tax Administration

Background

The Internal Revenue Service (IRS) uses Microsoft® Active Directory (AD) services for many information technology needs, which include secure user logon; access authorization; and credential validation for Windows laptops, desktops, and servers for all IRS employees, contractors, and business applications that interact with these computers.[1] Microsoft AD is a Windows domain service that blends authentication, authorization, and directory technologies to create enterprise security boundaries that are highly scalable. Microsoft AD 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. It simplifies system administration and provides methods to strengthen and consistently secure computer systems.

Additional benefits of AD's centralized management of computers and users include:

- A central location for network administration and security.
- The ability to scale up or down easily.
- Synchronization of directory updates across servers.
- The ability to design and deploy enterprise monitoring tools and security solutions.
- Centralized and consistent identity and authentication management.

In June 2018, we reported[2] that the IRS needed to improve its AD oversight and that Criminal Investigation lacked minimum security controls to protect data. The Active Directory Technical Advisory Board (ADTAB) should oversee any changes in the AD architecture, but we found that the ADTAB did not meet the basic requirements of its charter and did not provide adequate governance or oversight of the AD architecture.

Although we focused on Criminal Investigation's AD implementation in our previous audit, during planning and fieldwork we observed security deficiencies in computer rooms housing some Integrated Submission and Remittance Processing (ISRP) domain controllers. The ISRP AD forests exist to support the ISRP system, which converts paper tax documents, information documents, and remittances received into electronic records of taxpayer data. The system collects and stores Sensitive But Unclassified taxpayer data including but not limited to taxpayer

[1] See Appendix V for a glossary of terms.
[2] Treasury Inspector General for Tax Administration, Ref. No. 2018-20-034, *Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls* (June 2018).

name, address, and banking and payment information. Security weaknesses in the AD could allow unauthorized access to critical IRS servers, applications, and account management.

This review was performed during the period of March through September 2019 at the following locations: IRS Campuses in Fresno, California; Covington, Kentucky;[3] Kansas City, Missouri; Austin, Texas; and Ogden, Utah (to include the Main Building and the Arka Building). We worked closely with the Information Technology organization's Applications Development, Enterprise Operations, and Cybersecurity functions and with the Facilities Management and Security Services organization. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Detailed information on our audit objectives, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[3] As of August 2019, the ISRP system and supporting AD forest at the Covington, Kentucky, location was shut down permanently.

Results of Review

The Active Directory Technical Advisory Board Implemented Prior Recommendations

In June 2018, the IRS agreed to review the scope of the ADTAB's defined oversight responsibilities and modify it as necessary to ensure that the ADTAB is providing enterprise-wide oversight of the AD architecture, including the AD forests that operate outside of the Enterprise Operations function. Further, the IRS agreed to update its ADTAB charter and ensure that all individual forest owners are appropriately represented on the ADTAB. The ADTAB generally implemented all of our previous recommendations. In March 2019, the board updated its charter to align its responsibilities with its activities. The board also added voting and non-voting members, ensuring that all AD forest owners are represented on the board.

Computer Rooms for Integrated Submission and Remittance Processing Domain Controllers Lack Physical Security Controls

We conducted site visits at six locations to evaluate the physical security controls protecting the computer rooms housing ISRP domain controllers.[4] We evaluated the physical security controls including environmental protections, fire safety and suppression, temperature and humidity controls, emergency power sources and shutoff switches, and multifactor authentication.

The National Institute of Standards and Technology (NIST)[5] sets guidelines for conducting assessments of security controls and privacy controls employed within Federal information systems and organizations. The Internal Revenue Manual (IRM)[6] establishes the responsibilities for the physical security programs designed to protect IRS personnel, assets, and information. The IRM also states the policy for implementation, management, and security of information systems.[7] The IRS is required to designate as Limited Areas rooms that house information technology assets such as, but not limited to, mainframes, servers, associated peripherals, and communications equipment. In addition, the IRM sets the policy on minimum baseline security requirements designed to protect the critical infrastructure and assets against attacks that exploit assets, prevent unauthorized access to assets, and enable computing environments that support

[4] The ISRP supports seven IRS locations; however, only the six locations visited housed ISRP AD domain controllers.
[5] NIST Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* (Dec. 2014).
[6] IRM 10.2.1, *Physical Security* (Sept. 27, 2017).
[7] IRM 10.8.1, *Information Technology Security, Policy, and Guidance* (May 9, 2019).

the business needs of the organization. Further, the Occupational Safety and Health Administration sets regulations for fire safety and protection.

We found 15 physical security violations related to these controls. Figure 1 summarizes the physical security policy violations we found in the computer rooms with ISRP domain controllers.

Figure 1: Summary of ISRP Computer Room Physical Security Violations

Physical Security Control Area	Number of Policy Violations
Fire Safety and Suppression	2
Emergency Power Sources and Shutoff	1
Limited and Critical Areas	6
Multifactor Authentication	6
Total	**15**

Source: Treasury Inspector General for Tax Administration (TIGTA) analysis of information collected during site visits conducted from April through May 2019.

Stand-alone fire extinguishers

The Occupational Safety and Health Administration[8] requires agencies to distribute portable fire extinguishers for use by employees so that the travel distance for employees to any extinguisher is 75 feet or less. It also requires portable extinguishers to be visually inspected monthly. During our review, we observed a physical security weakness related to portable fire extinguishers at one of the six sites visited. Specifically, the fire extinguisher in the computer room at the Arka Building was not inspected on a monthly basis.

Fire suppression systems

The IRM states that automatic fire detection and suppression systems powered by independent energy sources are required for facilities that are not continually staffed. The Occupational Safety and Health Administration[9] further requires the IRS to test the main drain flow and the inspector's test valve of these automatic fire suppression systems, annually and biannually, respectively. All of the sites we visited annually tested the automatic fire suppression systems, but one site failed its most recent annual test. The Fresno Campus failed its annual fire suppression system test because multiple devices from a previous system needed to be either

[8] U.S. Department of Labor, Occupational Safety and Health Standards 1910.157, *National Fire Protection Association Standard No. 10* (Nov. 2002).
[9] U.S. Department of Labor, Occupational Safety and Health Standards 1910.159, *Automatic Sprinkler Systems* (May 1, 1981).

removed or connected to the new system. The fire suppression system test report did not specify which of the two possible actions the IRS needs to complete to resolve the failure.

Emergency power shutoff

We found a disabled emergency power shutoff switch at one of the six locations visited. The IRM states that the IRS shall:

- Provide the capability of shutting off power to an information system or individual system components in emergency situations.
- Place emergency shutoff switches or devices in a location near an information system or system component to facilitate safe and easy access for personnel.
- Protect the emergency power shutoff capability from unauthorized activation.

In the computer room in the Arka Building, the emergency power shutoff switch was disabled by a large paper clip purposefully lodged behind it, not allowing the switch to be engaged. In addition, the shutoff switch was covered with a piece of paper. These same conditions existed more than two years ago during fieldwork for our prior AD audit.

Limited Areas

The IRM[10] defines a Limited Area as an area limited to authorized personnel with a verified business need for entry. The IRM also states that:

- Only individuals assigned to the area will be provided a Limited Area Personal Identity Verification (PIV) card containing the "R" indicator, which signifies an individual assigned to a Limited Area. Note: The PIV card is encoded with permission to access a Limited Area. The "R" on the PIV card is a visual indicator showing an individual's assignment to a Limited Area.
- Form 5421, *Limited Area Register*, will be maintained at the main entrance to the Limited Area. Each person entering the Limited Area who is not assigned to that area will sign the register.
- The Limited Area manager must approve all names added to the authorized access list. The authorized access list will be prepared monthly and will be dated and signed by the manager.
- At the end of each month, the Limited Area manager will review the authorized access list and the Form 5421 and forward them to the local physical security office for review and to modify access, as appropriate.

[10] IRM 10.2.14, *Methods of Providing Protection* (Aug. 17, 2016).

We found six violations of the Limited Area policies in three of the six locations visited. For example, personnel with access to the Kansas City Campus computer room did not have PIV cards with the required "R" indicator. We observed an employee on site in the computer room without an "R" indicator on the PIV card, and when we asked about the lack of an "R" indicator, they said they were unaware that it was a policy violation. When we reviewed the Authorized Access Lists for that site, we found they were tracking which personnel did not have "R" PIV cards. However, the same personnel needed "R" indicator cards for at least two consecutive months with no resolution.

During our May 2019 visits, the computer rooms in the Kansas City Campus and the Austin Campus did not have Forms 5421 for visitors to sign. In addition, we reviewed the May 2019 Authorized Access List for the Austin Campus computer room and were provided no evidence that the list was reviewed monthly and updated in accordance with the IRM.

Based on our review, we determined computer rooms housing ISRP domain controllers lacked management oversight to ensure that Federal and IRM requirements are met. Without properly secured computer rooms, the IRS is operating with a significantly increased risk of attack. A compromised domain controller can be modified offline and placed back on the IRS network. As a result, the IRS cannot ensure that sensitive taxpayer information is being adequately protected.

Critical areas

The IRM classifies computer rooms as critical areas.[11] As such, computer rooms are secured, Limited Areas and access must be controlled in accordance with Limited Area standards. We found that one of six computer rooms housing an ISRP domain controller was not properly secured. In the Arka Building, an ISRP domain controller is housed in a locked cabinet located in a computer room that is part of a greater Limited Area for submission processing operations. The computer room also contains a printer and mail sorter. However, the door to the computer room is unlocked, which allows all visitors and employees with access to the larger processing area uncontrolled access to the computer room where the ISRP domain controller is located.

Because the IRS collocated submission processing operations equipment within the computer room, the room is unlocked and accessible by personnel who do not need access to an ISRP domain controller. IRS personnel stated they disabled the emergency power shutoff switch in the computer room because untrained personnel were pressing the switch, thinking it opened the computer room door. Without separating the computer room from submission processing operations equipment, the IRS cannot control the movement of individuals and eliminate unnecessary traffic through this critical security area and reduce the opportunity for unauthorized disclosure or theft of tax information.

[11] IRM 10.2.11, *Basic Physical Security Concepts* (Sept. 4, 2019).

Multifactor authentication not implemented for Limited Areas

Multifactor authentication has not been implemented for any of the Limited Area computer rooms located in the six IRS locations that we visited. We reported similar results in our June 2018 AD audit report in which we identified eight Criminal Investigation computer rooms that were not accessed via multifactor authentication. The NIST defines the designations of "Controlled," "Limited," or "Exclusion" to be applied to protected areas.[12] The NIST also outlines the number of authentication factors needed to access each designation. For Limited Areas such as computer rooms, two authentication factors are required.

Five of the six computer rooms containing ISRP domain controllers were accessed via card reader. The card readers used at these rooms authenticate the identity of an individual using a PIV card, which serves as single authentication factor. The computer room in the Arka Building was not secured from employees who have access to the larger submission processing area. This larger area is accessed using a single authentication factor, which is not in accordance with NIST requirements.

The IRS did not implement multifactor authentication for the Limited Area computer rooms we visited because the current access control system does not allow for multifactor authentication. According to Facilities Management and Security Services personnel, the IRS is in the process of upgrading the software and hardware for the Enterprise Physical Access Control System. The software is being upgraded to a version that is compatible with multifactor authentication, and all IRS facilities should have the necessary software version by June 2020. They also stated the hardware upgrade will take longer because it is dependent on funding from the Cybersecurity function. According to Facilities Management and Security Services personnel, the Cybersecurity function provided $3.2 million in Fiscal Year 2019 for this effort. With about 80 locations still needing upgraded hardware, the estimated timeline for completion is approximately three more years.

Without adequate access controls, such as multifactor authentication, the IRS increases the risk of unauthorized individuals gaining access to information technology assets. The Kansas City Campus will be the only site housing an ISRP domain controller to have multifactor authentication in place by the end of Fiscal Year 2020. The current funding and schedule increase the risk of unauthorized access to taxpayer data.

Recommendations

The Chief Information Officer should:

Recommendation 1**:** Coordinate with Facilities Management and Security Services to ensure that computer rooms housing ISRP domain controllers are immediately updated to comply with

[12] NIST Special Publication 800-116, *A Recommendation for the use of PIV Credentials in Physical Access Control Systems* (June 2018).

IRM and Federal requirements for Limited Areas, fire safety and suppression, and emergency power.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief, Facilities Management and Security Services, in coordination with the Chief Information Officer, will ensure that all computer rooms housing ISRP domain controllers are updated to comply with IRM and Federal requirements for Limited Areas, fire safety and suppression, and emergency power.

Recommendation 2**:** Physically separate the submission processing equipment from the ISRP domain controllers and enforce access standards for critical areas.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief, Facilities Management and Security Services, in coordination with the Chief Information Officer, will ensure the physical separation of the submission processing equipment from the ISRP domain controllers and enforce access standards for critical areas.

Recommendation 3: Prioritize all computer rooms housing ISRP domain controllers for access control upgrades to ensure that these rooms are compliant with Federal multifactor authentication requirements.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief Information Officer will prioritize all computer rooms housing ISRP domain controllers for access control upgrades to ensure that these rooms are compliant with Federal multifactor authentication requirements.

The Integrated Submission and Remittance Processing Active Directory Architecture Lacks Necessary Logical Security Controls

Along with checking the physical security controls protecting domain controllers, we also tested the logical security controls. We evaluated whether the ISRP domain controllers have adequate protection from malicious code and vulnerabilities. In addition, we evaluated domain controller configuration compliance and tested the ISRP AD forest user account compliance with IRS policy requirements. We also considered architecture administrative costs.

Architecture administration

The IRS did not assess the current ISRP AD architecture to potentially reduce the administrative costs and digital footprint of operating multiple AD forests. Applications Development function personnel stated that each ISRP system currently needs a separate AD forest because the system can only communicate across a local area network. Further, they explained that restructuring the ISRP AD architecture would require a full system redesign. The IRS did not estimate potential system redesign costs. Without a system redesign estimate, we could not determine whether

there would be any cost savings when consolidating the ISRP AD architecture into a single forest once these system redesign expenses were considered.

Vulnerability scanning and protection from malicious code

Based on our evaluation, the IRS has implemented necessary tools to detect software vulnerabilities. The IRM requires system owners to deploy vulnerability scanning tools that look for software flaws and improper configurations and measure vulnerability impacts. The IRM also requires information systems such as domain controllers to be scanned at least monthly for vulnerabilities. Their vulnerability scanning tool can obtain a set of administrator-level credentials to log into a host when performing a scan. Scans which use these credentials are called credentialed or authenticated scans. There are several significant advantages to scanning a host while authenticated to the host.

- Scans reveal much more information about what is running on the hosts which leads to testing for more vulnerabilities.
- Scans are more accurate with a lower rate of false positives.
- For Windows scans, credentials will give access to the registry, which is required by many vulnerability checks.

The IRM requires that systems implement privileged access authorization to all information system components for selected vulnerability scanning activities to facilitate more thorough scanning. We requested reports showing credentialed vulnerability scan information for all 11 ISRP domain controllers. The IRS provided two vulnerability scan reports showing a credential scan date of May 30, 2019, for all domain controllers.

During our review of the first vulnerability scan report, we found that the IRS was not performing credentialed vulnerability scans prior to our request. Prior to TIGTA's request for credentialed vulnerability scans, we found:

- The IRS did not perform credentialed vulnerability scans on 6 of the 11 ISRP domain controllers since January 2018.
- The IRS did not perform credentialed vulnerability scans on 2 of the 11 ISRP domain controllers since November 2018.
- The IRS did not perform credentialed vulnerability scans on 3 of the 11 ISRP domain controllers since December 2017.

When the IRS performed the credentialed vulnerability scan, it resulted in a 312 percent increase in the vulnerabilities identified from the uncredentialed scan. We asked Cybersecurity function personnel why they did not perform credentialed scans prior to our request on May 30, 2019. Cybersecurity function personnel stated they needed to review vulnerability scan reports regularly to ensure that credentialed scans are successful. Applications Development function

personnel stated that they did not have policies and procedures to review the reports for credentialed scans. Without a vulnerability scan report review process to ensure that credentialed scans are completed, they were unable to identify whether the service accounts used to facilitate credentialed vulnerability scans had expired.

Remediation process

As part of the remediation process, the Cybersecurity function performs vulnerability scans monthly and submits the scan reports to the Applications Development function for review. The IRM requires the IRS to analyze vulnerability scan reports. We reviewed the second vulnerability scan report to assess the remediation process. We found 377 critical and high vulnerabilities across 11 ISRP domain controllers with a publication date as early as 2015.

Applications Development function personnel stated they rely on the ISRP contractor to analyze vulnerability scan reports. We reviewed the ISRP contract, and there is no requirement for the contractors to review vulnerability scan reports. The IRS provided guidance dated December 2018 for reviewing vulnerability scan reports; however, the Applications Development function did not follow the guidance in place. Without evaluating the vulnerability scan reports, the IRS cannot determine whether identified vulnerabilities are remediated.

Untimely remediation caused excessive vulnerabilities on one ISRP domain controller

We reviewed the second vulnerability scan report, which showed limited historical information such as first seen, last seen, last scan date, and remediation status. The first and last seen dates allowed us to determine previous scan dates. We found that 245 of the 377 critical and high vulnerabilities were on one domain controller with 167 of the 245 vulnerabilities categorized as critical and 78 of the 245 vulnerabilities categorized as high. When we discussed the number of critical and high vulnerabilities on the specific ISRP domain controller with IRS personnel, they said in July 2018 system administrators were unsuccessful in installing a monthly patch.

System administrators did not submit a help desk ticket for the unsuccessful patch installation, but notified the Applications Development function and ISRP contractors via e-mail. However, Applications Development function personnel failed to follow up to ensure that the domain controller was properly patched. Without timely remediation of vulnerabilities, the IRS significantly lessens its ability to reduce or eliminate the potential for exploitation of known vulnerabilities and to save on the resources otherwise needed to respond to incidents after exploitation has occurred.

Malicious code protection

In addition to vulnerability scanning and remediation, the IRS is required to protect information systems from malicious code. Malicious code protection mechanisms shall be updated whenever new releases are available in accordance with IRS configuration management policy and

procedures and shall be configured to perform weekly scans. We worked with ISRP system administrators, using an antivirus management console, to evaluate these requirements for the ISRP domain controllers and reviewed a report showing that all domain controllers were up to date with antivirus malicious code protection, and the virus definitions did not exceed 24 hours. All scans were dated within a week of the date that the IRS ran the report.

Windows Policy Checker

Windows Policy Checker is an application that validates applicable IRM security requirements on computers that use the Microsoft Windows operating system. Windows Policy Checker scans security settings on a target computer and records any noncompliant setting in one or more result files. We reviewed the Windows Policy Checker scans and reports for the ISRP domain controllers and found that all domain controllers had an average score of 83.25 percent but failed due to high-risk checks. According to the Windows Policy Checker User Manual, regardless of calculated compliance percentage, any computer that fails for high-risk checks will be classified noncompliant, presenting a serious risk.

Further, we found that the Windows Policy Checker itself is out of date. The IRS's current version of Windows Policy Checker was released in December 2014. It uses Security Technical Implementation Guidelines set by the Defense Information Systems Agency that are more than five years old. The most current Security Technical Implementation Guidelines for AD domain controllers were released in February 2019. The current Windows Policy Checker is still in use because the IRS provided interim guidance allowing IRS organizations to use the Windows Policy Checker until January 1, 2020, in preparation for a new security compliance checker.[13] The IRS cannot provide relevant and timely continuous monitoring with an application so outdated. The IRS will be unable to effectively assess or analyze security controls and security risks to support organizational risk-based decisions because it is using outdated standards.

Account controls

The IRM requires information systems to uniquely identify and authenticate organizational users or processes acting on behalf of organizational users. We reviewed ISRP AD forest settings governing account password and lockout policies and found that they were generally compliant with current IRM requirements. We found one area of deviation from IRM policies, but determined that the effect is minimal.

Authentication with the PIV card is required for access to all systems. The IRM also requires information systems to enforce password minimum and maximum lifetime restrictions. Business role accounts must be disabled, quarantined, or removed after a prescribed number of days of

[13] IRS Interim Guidance, Policy Update IRM 10.8 Section 1, *Information Technology Security, Policy and Guidance – Extension of Effective Dates for Technical Policies* (June 30, 2019).

inactivity in accordance with the IRM policy. Figure 2 shows the total number of service and business role account policy violations we found in the ISRP AD forests.

Figure 2: Summary of Account Policy Violations

Policy Violations	Number of Violations
Enabled service account passwords set to not expire.	51
Enabled business role accounts that have passwords set to never expire.	2,016
Enabled business role accounts are not required to use PIV card.	2,648
Enabled business role accounts have not reset passwords in 90 days.	2,194
Enabled business role accounts are not properly disabled.	1,729
Business role accounts are not properly placed in quarantine.	2,400
Business role accounts are not properly removed.	5,154
Total Policy Violations	**16,192**

Source: TIGTA analysis of information collected from the Users and Computers feature within the AD using PowerShell®.

The Enterprise Operations function is responsible for administering service and business role accounts. These violations occurred because the Enterprise Operations function is not effectively enforcing policy governing service and business role accounts. Attackers frequently discover and exploit legitimate but inactive business role accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for IRS network monitoring tools. Terminated contractor and employee accounts have often been misused in this way. This places IRS data at risk for loss, manipulation, and other unauthorized access.

Domain Admin group

We reviewed Domain Admin group membership as part of our audit. Microsoft states that Domain Administrators are all powerful within their domains. Some of the privileges granted to Domain Admin group members are adding workstations to a domain, forcing a shutdown from a remote system, managing auditing and security logs, taking ownership of files or other objects, and impersonating a client after authentication. If the IRS delegates permissions properly, Domain Admin group membership should be required only in situations in which an account needs high levels of privilege.

As we reviewed the membership of the Domain Admin group for the five production forests, we found:

- Multiple instances in the Domain Admin groups in which more than one account appeared to belong to a single employee. In these cases, we identified nearly identical

account names, one with an added suffix and one without. The IRS concurred that there are numerous times when a single user has at least two accounts.

- Accounts that lack the administrative suffix to differentiate between a business role account and a privileged account. The IRS concurred, stating that there are opportunities to improve usage of suffixes when naming standards change.
- Various naming methods deployed to denote a privileged account. The IRS concurred, stating that it will work to reconcile existing accounts and ensure they follow standards.
- Business role accounts inappropriately assigned in the Domain Admin group.

The IRM states system administrators shall have two business role accounts, one for administrator duties and one for general user activity. Also, non-privileged users shall be prevented from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards and countermeasures. By having multiple accounts belonging to a single user in the Domain Admin group, the IRS allows business role accounts to execute privileged functions. When elevated access is persistent or elevated privilege accounts use the same credentials to access multiple resources, a compromised account can result in a major breach.

There is no single standard to identify and distinguish accounts as administrator accounts. This causes administrators of each ISRP AD forest to decide, ad hoc, which accounts will be given Domain Admin privileges and how naming standards are applied. If an application that has too many privileges is compromised, the attacker might be able to expand the attack beyond what it would if the application had been under the least amount of privileges possible.

Recommendations

The Chief Information Officer should:

Recommendation 4**:** Ensure that the Applications Development function follows procedures for conducting reviews of the vulnerability scan reports and establishes procedures for verifying and reviewing credentialed vulnerability scan reports.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief Information Officer will ensure that procedures for conducting reviews of the vulnerability scan reports and establish procedures for verifying and reviewing credentialed vulnerability scan reports are followed.

Recommendation 5: Ensure that service account passwords for the vulnerability scanning tool are reset, as needed, to allow for credentialed scans and regularly complete credentialed scans for ISRP domain controllers.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief Information Officer will ensure that service account passwords for the vulnerability

scanning tool are reset to allow for credentialed scans and regularly complete credentialed scans for ISRP domain controllers.

Recommendation 6: Ensure that the Enterprise Operations function follows the established processes and procedures to remediate all critical and high vulnerability scan findings.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief Information Officer will ensure that all processes and procedures will be followed to remediate critical and high vulnerability scan findings for the ISRP AD enclave.

Recommendation 7: Ensure that application compliance checkers use up-to-date guidelines to provide recognized, standardized, and established benchmarks that stipulate contemporary secure configuration settings.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will deploy the capability to monitor security configurations based upon contemporary standards. The capability will be delivered by Continuous Diagnostics and Mitigation tools using current Defense Information Systems Agency Security Technical Implementation Guide checklists to monitor device configurations.

Recommendation 8: Review all business role accounts in the ISRP AD forests and ensure that they are in compliance with IRM policy regarding account disabling, quarantining, and removal.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief Information Officer will review all business role accounts in the ISRP AD forests and ensure that they are following IRM policy regarding account disabling, quarantining, and removal.

Recommendation 9: Ensure that business role account passwords are appropriately configured to expire and require that PIV cards be used in accordance with policy.

> ***Management's Response:*** The IRS agreed with recommendation. The Chief Information Officer will ensure that business role account passwords are appropriately configured to expire in accordance with policy. The Chief Information Officer will also require that PIV cards be used in accordance with policy by embarking on an architecture study to determine the right solution, and the IRS will initiate and complete the project based on the solution selected.

Recommendation 10: Ensure that service account passwords are appropriately configured to expire.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief Information Officer will ensure that service account passwords are appropriately configured to expire.

Recommendation 11: Review the Domain Admin groups in each ISRP AD forest and ensure that system administrators have only one privileged account and additional accounts belonging to a single user are removed.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief Information Officer will review the Domain Admin groups in each ISRP AD forest so that system administrators have only one privileged account and additional accounts belonging to a single user are removed.

Recommendation 12: Create a privileged account naming standard for the ISRP AD forests to distinguish a general business role account from a privileged account and ensure that these accounts are granted only Domain Admin group rights or other administrative level rights.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief Information Officer will create a privileged account naming standard for the ISRP AD forests to distinguish a general business role account from a privileged account so that these accounts are granted only Domain Admin group rights or other administrative level rights.

Appendix I

Detailed Objectives, Scope, and Methodology

Our overall objectives were to review the ADTAB's effectiveness in implementing our previous recommendations and to evaluate the effectiveness and efficiency of ISRP[1] AD implementation. To accomplish our objectives, we:

I. Reviewed the effectiveness of the ADTAB's implementation of our previous recommendations.[2]

- A. Reviewed the Joint Audit Management Enterprise System to identify the corrective actions the IRS planned to take to address our prior audit recommendations.
- B. Interviewed members of the ADTAB to determine whether they made effective changes to implement the recommendations.
- C. Obtained and reviewed evidence to support changes made by the ADTAB to address these recommendations.

II. Evaluated the ISRP AD forests domain controllers to determine whether they meet the minimum baseline security controls established by Federal guidance and IRS policy.

- A. Obtained and evaluated Group Policy Objects and relevant reports for the ISRP forests to determine whether they properly meet criteria.
- B. Obtained and reviewed lists of ISRP group, service, and business roles accounts in the AD to determine whether they properly adhere to IRM policies and best practices.
- C. Obtained, reviewed, and evaluated Windows Policy Checker outputs for the ISRP domain controllers.

III. Evaluated the effectiveness of physical security policies and procedures and environmental protections at ISRP sites where domain controllers reside.

- A. Determined and reviewed the IRM and NIST publications to evaluate physical security controls.
- B. Evaluated environmental protections and assessed against relevant IRM and NIST publications.

[1] See Appendix V for a glossary of terms.
[2] TIGTA, Ref. No. 2018-20-034, *Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls* (June 2018).

C. Evaluated physical access controls and assessed their adequacy against relevant IRM and NIST publications.

IV. Determined whether proper controls are in place to discover and remediate vulnerabilities and malicious code on ISRP domain controllers.

A. Reviewed vulnerability scans for ISRP domain controllers.

B. Determined whether the IRS properly remediates vulnerabilities.

C. Reviewed anti-malware protection on ISRP domain controllers.

V. Determined whether the Enterprise Operations function assessed the current ISRP AD architecture to reduce its digital footprint and reduce administrative costs.

A. Interviewed appropriate personnel to determine what options they evaluated, if any.

B. Obtained and reviewed any existing plans for ISRP AD architecture consolidation and expected cost savings.

C. Interviewed ADTAB members to determine the level of oversight given to potential AD consolidation efforts.

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 objectives: NIST requirements for security and privacy of Federal information systems and IRM policies related to physical and environmental security controls. We evaluated these controls through interviews with personnel from the Applications Development, Enterprise Operations, and Cybersecurity functions and Facilities Management and Security Services and reviews of relevant documentation provided by the IRS. We also examined reports developed from scans using the Windows Policy Checker application, vulnerability scanning tool, and antivirus management console. We extrapolated data to evaluate AD users, groups, Group Policy Objects, and other various AD elements using PowerShell scripts.

Appendix II

Major Contributors to This Report

Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Jena Whitley, Director
Jason McKnight, Audit Manager
Andrea Nowell, Lead Auditor
Khafil-Deen Shonekan, Senior Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Chief, Facilities Management and Security Services
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Applications Development
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Director, Cybersecurity Operations
Director, Submission Processing
Director, Enterprise Audit Management

Appendix IV

Outcome Measure

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

Type and Value of Outcome Measure:

- Protection of Resources – Potential; six IRS computer rooms with ISRP[1] domain controllers are potentially at risk because access is not controlled with multifactor authentication (see page 3)

Methodology Used to Measure the Reported Benefit:

We met with Enterprise Operations function personnel to determine the number and location of ISRP production domain controllers. We visited six IRS campuses with computer rooms that house ISRP domain controllers and conducted physical walkthroughs of the computer rooms to assess the physical security controls. We found that none of the computer rooms controlled access using the appropriate number of authentication factors as required by NIST 800-116.[2]

[1] See Appendix V for a glossary of terms.
[2] NIST Special Publication 800-116, *A Recommendation for the use of PIV Credentials in Physical Access Control Systems* (June 2018).

Appendix V

Glossary of Terms

Term	Definition
Antivirus	Detects, prevents, and removes viruses, worms, and other malware from a computer. Antivirus programs include an automatic update feature that permits the program to download profiled or new viruses, enabling the system to check for new threats.
Authentication	Verifies the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
Continuous Diagnostics and Mitigation	A program providing cybersecurity tools, integration services, and dashboards to participating agencies to support them in improving their respective security posture.
Critical Areas	Areas that, if damaged or compromised, could have significant adverse consequences for the IRS agency's mission or the health and safety of individuals within the building or the surrounding community.
Defense Information Systems Agency	A combat support agency that provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations.
Domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.
Domain Controller	A server that is running a version of the Windows Server operating system and has AD Domain Services installed.

Term	Definition
Forest	A complete instance of an AD. Each forest acts as a top-level container in that it houses all domain containers for that particular AD instance.
Integrated Submission and Remittance Processing	A system that converts paper tax and information documents and remittances received by the IRS into perfected electronic records of taxpayer data.
Joint Audit Management Enterprise System	The Department of the Treasury system for use by all bureaus to track, monitor, and report the status of internal control audit results. This system tracks specific information on issues, findings, recommendations, and planned corrective actions from audit reports issued by oversight agencies, such as TIGTA.
Limited Area	An area in a building where access is limited to authorized personnel only. All who access a Limited Area must have a verified official business need to enter. Limited Area space can be identified by the Chief, Facilities Management and Security Services Physical Security Section, based on critical assets.
Malicious Code (Malware)	Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. It can be a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Multifactor Authentication	Authentication using two or more factors to achieve authentication. Factors include: i) something you know, ii) something you have, iii) something you are.
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 agency operations and assets.
Patch	A software component that, when installed, directly modified files or device settings related to a different software component without changing the version number or release details for the related software component.

Term	Definition
Personal Identity Verification Card	A physical artifact, *e.g.*, identity card, "smart" card, issued to an individual that contains stored identity credentials, *e.g.*, photograph, cryptographic keys, digitized fingerprint representation, such that a claimed identity of the cardholder may be verified against the stored credentials by another person or an automated process.
PowerShell®	A task-based, command-line shell and scripting language built on.NET that helps system administrators and power users rapidly automate tasks that manage operating systems and processes.
Scalable	Capable of being easily expanded or upgraded on demand.
Security Technical Implementation Guidelines	Based on Department of Defense policy and security controls. Implementation guides are geared to a specific product and version. They contain all requirements that have been flagged as applicable for the product.
Vulnerability	A weakness in an information system, system security procedures, internal controls, or an implementation that could be exploited or triggered by a threat source.
Windows Policy Checker	An application that validates applicable IRM security requirements on computers that use the Microsoft Windows operating system.

Appendix VI

Management's Response to the Draft Report

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

CHIEF INFORMATION OFFICER

January 02, 2020

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Acting, Chief Information Officer

SUBJECT: Response to Draft Report – Active Directory Oversight Needs Improvement (Audit #201920013) (e-trak #2020-18375)

Thank you for the opportunity to review and comment on the draft report and to meet with the audit team to discuss the contents. The Internal Revenue Service (IRS) is fully committed to enhancing our Active Directory Architecture.

We agree with the audit recommendations and have developed corrective actions to remediate the report findings. We have made significant progress, having successfully implemented all of TIGTA's previous recommendations. For example, based on the evaluation, TIGTA found we implemented the necessary tools to detect software vulnerabilities. In addition to vulnerability scanning and remediation, TIGTA also found in this limited analysis that all domain controllers were up to date with antivirus malicious code protection. We are also in the process of upgrading the software and hardware for the Enterprise Physical Access Control System, although this significant amount of work depends on funding with about 80 locations still needing upgraded hardware.

Attached is our corrective action plan describing how we plan to address your recommendations. Please note that some of the remediation actions will be multiple years and all remediations are dependent on appropriate funding.

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 a member of your staff may contact Cecil Hua, Director, Infrastructure Services, at (240) 613-4589

Attachment

Draft Audit Report – Review of the IRS's Active Directory Architecture
(Audit #201920013)

Recommendation 1: The Chief Information Officer should coordinate with Facilities Management and Security Services to ensure that computer rooms housing Integrated Submission and Remittance Processing (ISRP) domain controllers are immediately updated to comply with Internal Revenue Manual (IRM) and Federal requirements for Limited Areas, fire safety and suppression, and emergency power.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Facilities Management and Security Services, in coordination with the Chief Information Officer, will ensure that all computer rooms housing Integrated Submission and Remittance Processing (ISRP) domain controllers are updated to comply with Internal Revenue Manual (IRM) and Federal requirements for Limited Areas, fire safety and suppression, and emergency power.

IMPLEMENTATION DATE : June 15, 2020

RESPONSIBLE OFFICIAL(S): Chief, Facilities Management and Security Services

Recommendation 2: The Chief Information Officer should physically separate the submission processing equipment from the Integrated Submission and Remittance Processing (ISRP) domain controllers and enforce access standards for critical areas.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Facilities Management and Security Services, in coordination with the Chief Information Officer, will ensure the physical separation of the submission processing equipment from the Integrated Submission and Remittance Processing (ISRP) domain controllers and enforce access standards for critical areas.

IMPLEMENTATION DATE : June 15, 2020

RESPONSIBLE OFFICIAL(S): Chief, Facilities Management and Security Services

Draft Audit Report – Review of the IRS's Active Directory Architecture
(Audit #201920013)

Recommendation 3: The Chief Information Officer should prioritize all computer rooms housing Integrated Submission and Remittance Processing (ISRP) domain controllers for access control upgrades to ensure that these rooms are compliant with Federal multi-factor authentication requirements.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will prioritize all computer rooms housing Integrated Submission and Remittance Processing (ISRP) domain controllers for access control upgrades to ensure that these rooms are compliant with Federal multi-factor authentication requirements.

IMPLEMENTATION DATE : December 15, 2021

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

Recommendation 4: The Chief Information Officer should ensure that the Applications Development function follows procedures for conducting reviews of the vulnerability scan reports and establishes procedures for verifying and reviewing credentialed vulnerability scan reports.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The Chief Information Officer will ensure procedures for conducting reviews of the vulnerability scan reports and establish procedures for verifying and reviewing credentialed vulnerability scan reports are followed.

IMPLEMENTATION DATE: June 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Applications Development

Draft Audit Report – Review of the IRS's Active Directory Architecture
(Audit #201920013)

Recommendation 5: The Chief Information Officer should ensure that service account passwords for the vulnerability scanning tool are reset, as needed, to allow for credentialed scans and regularly complete credentialed scans for Integrated Submission and Remittance Processing (ISRP) domain controllers.

CORRECTIVE ACTION 5: The IRS agrees with this recommendation. The Chief Information Officer will ensure that service account passwords for the vulnerability scanning tool are reset to allow for credentialed scans and regularly complete credentialed scans for Integrated Submission and Remittance Processing (ISRP) domain controllers.

IMPLEMENTATION DATE: May 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Applications Development

Recommendation 6: The Chief Information Officer should ensure that the Enterprise Operations function follows the established processes and procedures to remediate all critical and high vulnerability scan findings.

CORRECTIVE ACTION 6: The IRS agrees with this recommendation. The Chief Information Officer will ensure that all processes and procedures will be followed to remediate critical and high vulnerability scan findings for the Integrated Submission and Remittance Processing (ISRP) Active Directory (AD) enclave.

IMPLEMENTATION DATE: August 15, 2020

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

Draft Audit Report – Review of the IRS's Active Directory Architecture
(Audit #201920013)

Recommendation 7: The Chief Information Officer should ensure that application compliance checkers use up-to-date guidelines to provide recognized, standardized, and established benchmarks that stipulate contemporary secure configuration settings.

CORRECTIVE ACTION 7: The IRS agrees with this recommendation. The IRS will deploy the capability to monitor security configurations based upon contemporary standards. The capability will be delivered by Continuous Diagnostics & Mitigation (CDM) tools using current Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) checklists to monitor device configurations.

IMPLEMENTATION DATE: May 15, 2020

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

Recommendation 8: The Chief Information Officer should review all business role accounts in the Integrated Submission and Remittance Processing (ISRP) Active Directory (AD) forests and ensure that they are in compliance with Internal Revenue Manual (IRM) policy regarding account disabling, quarantining, and removal.

CORRECTIVE ACTION 8: The IRS agrees with this recommendation. The Chief Information Officer will review all business role accounts in the Integrated Submission and Remittance Processing (ISRP) Active Directory (AD) forests and ensure that they are following Internal Revenue Manual (IRM) policy regarding account disabling, quarantining, and removal.

IMPLEMENTATION DATE: December 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Applications Development

Draft Audit Report – Review of the IRS's Active Directory Architecture
(Audit #201920013)

Recommendation 9: The Chief Information Officer should ensure that business role account passwords are appropriately configured to expire and require that Personal Identity Verification (PIV) cards be used in accordance with policy.

CORRECTIVE ACTION 9: The IRS agrees with recommendation:

1) The Chief Information Officer will ensure that business role account passwords are appropriately configured to expire in accordance with policy.

   IMPLEMENTATION DATE : December 15, 2020
   RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

2) The Chief Information Officer will require that Personal Identity Verification (PIV) cards be used in accordance with policy by embarking on an architecture study to determine the right solution and IRS will initiate and complete the project based on the solution selected.

   IMPLEMENTATION DATE : December 15, 2024
   RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

Recommendation 10: The Chief Information Officer should ensure that service account passwords are appropriately configured to expire.

CORRECTIVE ACTION 10: The IRS agrees with this recommendation. The Chief Information Office will ensure that service account passwords are appropriately configured to expire.

IMPLEMENTATION DATE: December 15, 2020

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

Draft Audit Report – Review of the IRS's Active Directory Architecture
(Audit #201920013)

Recommendation 11: The Chief Information Officer should review the Domain Admin groups in each Integrated Submission and Remittance Processing (ISRP) Active Directory (AD) forest and ensure that system administrators have only one privileged account and additional accounts belonging to a single user are removed.

CORRECTIVE ACTION 11: The IRS agrees with this recommendation. The Chief Information Officer will review the Domain Admin groups in each Integrated Submission and Remittance Processing (ISRP) Active Directory (AD) forest so that system administrators have only one privileged account and additional accounts belonging to a single user are removed.

IMPLEMENTATION DATE: June 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Applications Development

Recommendation 12: The Chief Information Officer should create a privileged account naming standard for the Integrated Submission and Remittance Processing (ISRP) Active Directory (AD) forests to distinguish a general business role account from a privileged account and ensure that these accounts are granted only Domain Admin group rights or other administrative level rights.

CORRECTIVE ACTION 12: The IRS agrees with this recommendation. The Chief Information Officer will create a privileged account naming standard for the Integrated Submission and Remittance Processing (ISRP) Active Directory (AD) forests to distinguish a general business role account from a privileged account so that these accounts are granted only Domain Admin group rights or other administrative level rights.

IMPLEMENTATION DATE: June 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Applications Development