TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls

June 27, 2018

Reference Number: 2018-20-034

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

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 AND CRIMINAL INVESTIGATION COMPUTER ROOMS LACK MINIMUM SECURITY CONTROLS

Highlights

Final Report issued on June 27, 2018

Highlights of Reference Number: 2018-20-034 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

Active Directory is a Microsoft Windows® domain service that blends authentication, authorization, and directory technologies to create enterprise security boundaries that are widely distributable and highly scalable. Security weaknesses in Active Directory could allow unauthorized personnel to gain access to critical IRS servers, applications, and account management.

WHY TIGTA DID THE AUDIT

This audit was initiated to review the IRS Active Directory Technical Advisory Board and evaluate the effectiveness of Criminal Investigation's (CI) Active Directory implementation.

WHAT TIGTA FOUND

TIGTA previously recommended that the IRS establish an agencywide Active Directory governing body that finalizes and enforces forest design criteria, develops standards, oversees trusts, and ensures that unauthorized forests or domains are not implemented. Although the IRS agreed to this recommendation, the governing body created in May 2013 is not providing agencywide Active Directory oversight.

During the review of CI's implementation of Active Directory, TIGTA found that computer rooms in CI field offices lack necessary physical security controls. Specifically, TIGTA identified a total of 88 physical security control weaknesses related to Limited Areas, two-factor authentication, control and safeguarding lock combinations, fire extinguishers, temperature and humidity controls, emergency power shutoff switches, and backup power sources.

The CI Active Directory architecture lacks necessary logical security controls. For example, the operating systems on the domain controllers are only 64 percent compliant with security requirements, and 295 service accounts and 1,751 user accounts are improperly configured. Finally, TIGTA found that the IRS's Windows Policy Checker is out of date and uses three-year-old technical guidelines to conduct its analysis.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer ensure that the Active Directory Technical Advisory Board is providing agencywide oversight and update its charter. Additionally, TIGTA recommended that the Chief, CI, with assistance from the Chief Information Officer, complete a cost analysis between relocating CI assets to IRS computer rooms versus upgrading CI computer rooms to meet Federal and internal security standards and implement the most cost-effective solution; ensure that CI computer rooms are immediately updated to comply with Federal and internal security requirements relating to Limited Areas, key and cipher lock combination controls, and stand-alone fire extinguishers while a cost-effective solution regarding the computer room location is identified and implemented; ensure that local personnel are properly trained; ensure that applications used as compliance checkers use up-to-date guidelines; ensure that Active Directory user accounts are in compliance with internal policy; and ensure that user accounts and service accounts are appropriately configured.

MANAGEMENT RESPONSE

The IRS agreed with all recommendations. The IRS plans to review the current scope of oversight responsibilities; identify the steps needed to comply with physical security requirements; conduct training; transition to the enterprise Continuous Diagnostics and Mitigation security configuration management solution; update its current manual process of disabling user accounts; and ensure that access to network or local resources uses multifactor authentication.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

June 27, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls (Audit # 201720019)

This report presents the results of our review of the Internal Revenue Service (IRS) Active Directory Technical Advisory Board and evaluation of the effectiveness of Criminal Investigation's Active Directory implementation. This audit is included in our Fiscal Year 2018 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

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

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

Abbreviations

AD	Active Directory
ADTAB	Active Directory Technical Advisory Board
CI	Criminal Investigation
ECC	Enterprise Computing Center
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
PIV	Personal Identity Verification

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 and all IRS employees, contractors, and business applications that interact with these computers.[1] AD is also used for the enforcement of Internal Revenue Manual (IRM) and operational standards to all Windows laptops, desktops, servers, user accounts, and service accounts. Microsoft AD is a Windows domain service that blends authentication, authorization, and directory technologies to create enterprise security boundaries that are highly scalable. AD also enables administrators to assign agencywide policies, deploy programs to many computers, and apply critical updates to an entire organization's systems simultaneously from a central, organized, accessible database. It simplifies system administration and provides methods to strengthen and consistently secure computer systems.

Additional benefits of centralized management of computers and users with AD include:

- 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 September 2011, we reported that the IRS did not enforce the centralization of its Windows environment. Centralization would simplify system administration and achieve consistent identity and authentication management, which is required by Federal regulations and IRS enterprise architecture security principles.[2] We found multiple organizations that maintained a total of 20 AD forests. A forest is the outermost design element or boundary in an AD implementation. As a general rule, best practices dictate that the use of multiple forests for a single application or business process should be avoided. Ideally, there should be only one forest in an organization for maximum administration, cost, and security efficiencies. Because each forest is administered separately, adding additional forests increases an organization's management overhead. The IRS spent $1.2 million in contract fees to maintain obsolete computer equipment in one of these groups rather than spending those funds to refresh their

[1] See Appendix IV for a glossary of terms.
[2] Treasury Inspector General for Tax Administration, Ref. No. 2011-20-111, *Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies* (Sept. 2011).

computer equipment. The IRS also did not ensure that all Windows computers connected to its network were authorized and compliant with security policy, putting the IRS at risk of security breaches. While the IRS had created standards to prevent unauthorized computers from being connected to the network, it had not established a central controlling authority to enforce compliance with its policy. We recommended that the IRS establish an agencywide AD governing body that finalizes and enforces forest design criteria, develops standards, oversees trusts, and ensures that unauthorized forests or domains are not implemented. The IRS agreed with this recommendation.

During the planning phase of our current review, we conducted a survey in order to identify and understand the AD architecture. As a result of this survey, we were able to obtain specific information regarding the IRS personnel responsible for forest administration, the AD architecture, the policies that govern AD and domain controllers, and the security tools and methodology used for policy enforcement. Based on the results of our planning survey, we determined that there are 19 active forests operating within the IRS. Figure 1 summarizes information about the 19 IRS AD forests.

Figure 1: Summary Information for the 19 AD Forests

Forest Name	Forest Owner (IRS organization)	IRS Organization That Operates and Maintains the Forest
DSDT	Enterprise Operations	Enterprise Operations
ADFED	Enterprise Operations	Enterprise Operations
ETJOC	Enterprise Operations	Enterprise Operations
IRSCounsel	Chief Counsel	Enterprise Operations
IRSNET	Enterprise Operations	Enterprise Operations
CI	Criminal Investigation (CI)	CI
ISRP (10 forests)	Integrated Submission and Remittance Processing	Integrated Submission and Remittance Processing
IRS.GOV	Research, Applied Analytics, and Statistics	Research, Applied Analytics, and Statistics
Geo-IRS	User and Network Services	User and Network Services
CSIRCNET	Cybersecurity	Cybersecurity

Source: Results obtained from Treasury Inspector General for Tax Administration survey of IRS forest owners conducted in April 2017.

Based on the number of IRS AD forests identified through our planning survey, we decided to judgmentally select a midsize forest for an in-depth review. We believe that one of the greatest risks is the lack of controls on the physical security of server rooms where domain controllers are

located in remote sites outside of the IRS Enterprise Computing Centers (ECC) and the IRS **********2**********. Therefore, we selected CI because it operates more independently from the Enterprise Operations organization than other forest owners and it houses several physical domain controllers at remote sites. This review was performed during the period May 2017 through February 2018 at:

- **********2**********.
- IRS ECCs located in **********2**********.
- IRS facilities located in the following Federal buildings/centers:
  - **********2**********.
  - **********2**********.
  - **********2**********.
  - **********2**********.
- IRS offices in the following cities:
  - **********2**********.
  - **********2**********.
  - **********2**********.
  - **********2**********.

During the site visits, we worked closely with IRS personnel from CI, Agency-Wide Shared Services, and Information Technology's Enterprise Operations and Cybersecurity organizations.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The Active Directory Technical Advisory Board Is Not Providing Agencywide Oversight

In September 2012, the IRS Infrastructure Executive Steering Committee modified its charter and approved the creation of an AD advisory board. The new governing body was approved to finalize and enforce forest design criteria and standards, oversee trusts, and ensure that unauthorized forests or domains are not implemented in the IRS. The initial AD Advisory Board charter was approved for implementation in September 2012 and subsequently revised, creating the AD Technical Advisory Board (ADTAB) in May 2013. The ADTAB has the authority to oversee any changes in the AD architecture and report them to the Infrastructure Executive Steering Committee for approval. If any IRS forest owner wants to modify their respective forest (*e.g.*, adding or removing a domain, adding domain controllers, or collapsing a forest) they are supposed to report to the ADTAB for approval.

Per the current ADTAB charter, the primary responsibilities of the ADTAB are to:

- Establish and maintain change control of a baseline of forests, domains, trusts, and Group Policy Object standards.
- Recommend and maintain AD forest design criteria.
- Oversee and report on compliance to the Infrastructure Executive Steering Committee for nonsecurity issues.
- Oversee and report on compliance to the Security Services and Privacy Executive Steering Committee for security issues.
- Oversee and recommend corrective actions for unauthorized forests or domains.

We interviewed ADTAB members, who told us that they did not know how many active forests currently exist within the IRS. They were also unable to provide any documentation that identified or summarized the various AD forest environments agencywide. The ADTAB holds monthly meetings to discuss the operational status and items related to the IRS AD architecture. We reviewed all of the ADTAB monthly meeting minutes from November 2015 through June 2017 to determine what oversight was performed.

In April 2017, CI upgraded its functional forest level from Microsoft Windows Server 2008 to 2012. Officials in CI could not produce any evidence that the ADTAB was made aware of or approved the upgrade as required. In another example, the IRS upgraded the Geo-IRS functional forest level twice within the past three years with no involvement from the ADTAB. In the

meeting minutes we reviewed, there is no record that any of these upgrades were discussed. Furthermore, according to IRS officials we interviewed, not all forest owners are members of the ADTAB, nor do all of them understand the mission of the ADTAB.

Based on the results of our review, the ADTAB did not meet the basic requirements of its charter. The ADTAB does not provide adequate governance or oversight of the IRS AD architecture. The scope of the ADTAB was never properly established and does not satisfy the intent of our original September 2011 recommendation.

Without proper agencywide oversight of Microsoft Windows technologies like AD, the IRS increases its risk of noncompliance with Federal and agency information technology policies and procedures. By operating 19 AD forests, the IRS is not taking advantage of security and operational efficiency benefits of centralized management of computers and users with AD. As a result, the IRS cannot ensure that sensitive taxpayer information and taxpayer dollars are preserved and protected. When IRS operations run securely and efficiency, it helps maintain taxpayer confidence, which is critical for the IRS to perform its mission.

Recommendations

The Chief Information Officer should:

Recommendation 1**:** Review the current scope of the ADTAB's defined oversight responsibilities and modify as necessary to ensure that the ADTAB is providing agencywide oversight of the AD architecture, including the AD forests that operate outside of the Enterprise Operations organization.

> ***Management's Response:*** The IRS agreed with this recommendation and plans to review the current scope of the ADTAB's defined oversight responsibilities and modify as necessary.

Recommendation 2: Update the existing ADTAB charter and ensure that all individual forest owners are appropriately represented on the ADTAB.

> ***Management's Response:*** The IRS agreed with this recommendation and plans to update the existing ADTAB charter and ensure that all individual forest owners are appropriately represented on the ADTAB.

Criminal Investigation Computer Rooms Lack Physical Security Controls

We conducted site visits at 11 IRS locations to review the physical security controls of the CI computer rooms housing domain controllers. Two of these locations were ECCs; one was the **********2**********; and the remaining eight were IRS field offices located throughout the United States.

The National Institute of Standards and Technology (NIST)[3] sets guidelines for conducting assessments of security controls and privacy controls employed within Federal information systems and organizations. The IRM[4] establishes the responsibilities for the IRS physical security programs designed to protect IRS personnel, assets, and information; it also[5] states the policy for implementation, management, and security of information systems within the IRS. The IRS is required to designate restricted areas 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 the business needs of the organization.

We evaluated the physical security controls, to include environmental protections, related to Limited Areas, two-factor authentication, control and safeguarding lock combinations, fire extinguishers, temperature and humidity controls, emergency power shutoff switches, and backup power sources. We found a total of 88 policy exceptions relating to physical security controls, with 87 (99 percent) of 88 of the exceptions observed at the eight field offices. We also found an existing IRS computer room located within each of these field offices, separate from the CI computer room housing its domain controllers. Figure 2 summarizes the physical security weaknesses, *i.e.*, policy exceptions, we found in the CI computer rooms.

Figure 2: Summary of CI Computer Room Physical Security Weaknesses

Physical Security Control Area	Number of Policy Exceptions
Limited Areas	51
Two-Factor Authentication	8
Control and Safeguarding Lock Combinations	5
Stand-Alone Fire Extinguishers	9
Temperature and Humidity Controls	1
Emergency Power Shutoff	7
Emergency Power	7
Totals	**88**

Source: Treasury Inspector General for Tax Administration analysis of information collected during site visits from May through December 2017.

[3] NIST, NIST Special Publication 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* (Dec. 2014).
[4] IRM 10.2.1, *Physical Security* (Sept. 27, 2017).
[5] IRM 10.8.1, *Information Technology Security, Policy, and Guidance* (July 8, 2015).

Limited Areas

We found that only two (25 percent) of eight field offices had properly designated their CI computer rooms as Limited Areas. The IRM[6] defines a Limited Area as an area to which access is limited to authorized personnel only and two-factor authentication will be required. The IRM also states that:

- Limited Areas will have signs prominently posted as "Limited Area."
- 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.
- 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.

Some of the on-site CI Computer Operations Administrators told us that they were not aware of the requirement to designate computer rooms as Limited Areas. On two separate occasions, Computer Operations Administrators took steps to correct this deficiency while we were on-site. The signs displayed at each of the two ECCs appropriately and prominently designated the computer rooms as Limited Areas.

None of the eight field offices issued PIV cards with the required "R" indicator. We found that ******2****** is not meeting the IRM requirement to issue PIV cards with the "R" indicator to all employees assigned to a Limited Area. While at ********2*********, we observed personnel who entered the designated Limited Area with no "R" indicator on their badge. Upon reporting this issue, IRS officials told us that the "R" indicator was a legacy holdover and no longer a valid requirement. We confirmed that the policy is still in place.

We found that Form 5421 was completely implemented, used, and properly retained at only one of the eight field offices. At the remaining seven field offices, we observed exceptions that included:

- Recent implementation due to "word of mouth" from one of our prior site visits.

[6] IRM 10.2.5, *Security, Privacy and Assurance, Physical Security Program, Identification Card* (Sept. 5, 2014).

- The most recent entries were greater than six months old; in one case, from 2010.
- Maintenance personnel were not signing the register.

Finally, approved access lists existed for only two of the field offices for the CI computer rooms. Of those two, one of the lists was extremely outdated and included unlimited access to the computer room by separated employees. We found no records at any of the eight field offices that documented the required monthly reviews of the authorized access list and the Limited Area register; therefore, this information was not forwarded on to the local security office for review and retention. We observed access management operations at each of the two ECCs that aligned with Federal and agency guidelines.

Two-factor authentication

Two-factor authentication has not been implemented for any of the CI computer rooms located in the eight field offices. The NIST defines the designations of "Controlled," "Limited," or "Exclusion," which should be applied to protected areas.[7] For Limited Areas such as computer rooms, two-factor authentication is required. The IRM agrees with the NIST requirements that a Limited Area is an area where access is limited to authorized personnel only and two-factor authentication is required.

The CI field offices are instead using the following methods to access the computer room: badge only, key, or cipher lock. We found two-factor authentication in place at each of the two ECCs and the *******2********, with one minor exception. The visitor badges issued for entry into the *******2******** computer rooms were not functioning properly. The IRS security guards told us that the visitor badges were not programmed to function in the same manner as the permanent employee badges.

Control and safeguarding of cipher lock combinations

We found combination locks to gain access to the CI computer rooms in five of the eight field office locations. For the five locations, none of the offices had a process in place to ensure that the locks were being changed in accordance with IRM policy.[8] The specific exceptions we observed included:

- Personnel were not aware of the IRM requirements relating to combination locks.
- One location was still using the manufacturer default as the combination.
- Other offices only changed the combination when employees departed the IRS.

[7] NIST, NIST Special Publication 800-116, *A Recommendation for the use of PIV Credentials in Physical Access Control Systems* (Nov. 2008).
[8] IRM 10.2.14, *Methods of Providing Protection* (Aug. 17, 2016).

The IRM states that access to a locked area, room, or container can only be controlled if the key, access card, or combination is controlled. As soon as the combination is obtained by an unauthorized person or otherwise compromised or the key is lost, the security provided by that particular lock is lost. According to the IRM, the combination to each lock will be changed:

- When the safe or lock is originally received.
- At least every three years.
- When a person knowing the combination no longer requires access to it and other controls do not exist to prevent their access to the lock.
- When the combination is compromised.

Stand-alone fire extinguishers

The Occupational Safety and Health Administration[9] requires the IRS 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 provides that portable extinguishers shall be visually inspected monthly. During our review, we observed nine policy exceptions relating to portable fire extinguishers at the eight field office locations, including:

- Two field offices did not have a portable fire extinguisher within the required distance of the CI computer room.
- Seven field offices were not meeting the monthly testing or visual inspection requirements, and, in one instance, the extinguisher was last tested in 2009.

Temperature and humidity controls

We observed acceptable temperature levels inside 10 of the 11 CI computer rooms. The IRM requires acceptable levels of temperature and humidity and requires continuous monitoring of these levels within the facilities where information systems reside. The temperature level at the one exception facility was 79 degrees at the time of our walkthrough. Based on this temperature and the Special Agent in Charge telling us that they occasionally open the computer room door to increase airflow, we determined this to be an exception to this control.

Emergency power shutoff

We observed emergency power shutoff switches at each of the ECCs and the Main building in *******2********. However, only one of the eight field office locations was equipped with an emergency power shutoff switch. The IRM states that the IRS shall:

[9] U.S. Department of Labor, Occupational Safety and Health Standards 1910.157(d)(2), (d)(4), and (e)(2), *National Fire Protection Association Standard No. 10* (Nov. 2002).

- 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.

Emergency power

We found that only one of the eight field offices was equipped with an external emergency power capability. Additionally, we observed several instances in which industry best practices for uninterruptible power supplies were not followed. For example, some displayed fault lights, and others were not plugged into a separate power source. The IRM requires a short-term uninterruptible power supply be provided to facilitate either an orderly shutdown of the information system or transition of the information system to a long-term alternate power in the event of a primary power loss.

Based on the comprehensive results of our review, CI computer rooms that are located in IRS field offices lack management oversight. The Computer Operations Administrators lack basic knowledge regarding IRS information technology policies and procedures. This lack of knowledge coupled with a lack of direct oversight make it difficult to operate and maintain a secure computer room in accordance with Federal and agency guidelines.

Further, during our audit planning, we inspected an IRS facility housing the ISRP domain controllers. This facility failed to meet basic safety and security requirements for sensitive information technology assets. Specifically, there was no lock on the door to access the computer room. At least one hundred employees have access to this room at any given time, and that number increases to over 300 seasonal employees during peak filing season. In addition, the emergency power shutoff switch was covered with a piece of paper and disabled with a paperclip. We did not include the policy exceptions found at this facility in the summary table above (Figure 2) because these assets are not owned by CI.

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.

Recommendations

The Chief, CI, with assistance from the Chief Information Officer, should:

Recommendation 3: Complete a cost analysis to 1) determine the efficacy of relocating CI assets in each of the field offices to existing IRS computer rooms versus upgrading the CI

computer rooms to ensure that assets are protected in accordance with Federal and IRM security requirements and 2) implement the most cost-effective solution.

> ***Management's Response:*** The IRS plans to collaborate with the Facilities Management and Security Services and Information Technology organizations to complete a joint analysis of each computer room in CI field offices within 12 months and determine the most effective and efficient course of action to meet Federal and IRM security standards. The joint analysis should address the technological, operational, physical location, funding, and time factors necessary to either relocate the assets to existing IRS computer rooms or bring the CI computer rooms into compliance. The joint cost analysis should then be the basis for a developing joint project plan to implement the proposed solutions contingent with the time needed to properly plan and fund the relocation of CI assets or secure those assets in the existing locations.

Recommendation 4***:*** Ensure that CI computer rooms are immediately updated to comply with IRM requirements for Limited Areas, key and cipher lock combination controls, and stand-alone fire extinguishers while a cost-effective solution regarding the computer room location is identified and implemented.

> ***Management's Response:*** The IRS agreed with this recommendation. Specifically, CI plans to partner with Facilities Management and Security Services to 1) identify the steps needed to comply with Limited Area access controls, safeguards for keys and lock combinations, and requirements for stand-alone fire extinguishers in CI computer room locations and 2) develop, within 12 months, a joint project plan to address these IRM requirements.
>
> ***Office of Audit Comment:*** We are concerned about the lack of urgency in implementing the basic physical security controls included in the recommendation. We do not believe it should take 12 months to develop a project plan to address the requirements.

Recommendation 5: Ensure that local Computer Operations Administrators are properly trained to understand and comply with IRS policies and procedures governing Limited Areas and provide oversight to ensure that these policies and procedures are kept current.

> ***Management's Response:*** The IRS agreed with the recommendation. Specifically, CI plans to conduct training for all Computer Operations Administrators on IRS policies and procedures governing Limited Areas and will ensure that these policies and procedures are followed.

The Criminal Investigation Active Directory Architecture Lacks Necessary Logical Security Controls

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

Vulnerability scanning and protection from malicious code

Based on our evaluation, we found that CI has successfully deployed the necessary tools and implemented procedures to detect software vulnerabilities and protect the domain controllers against malicious code. 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. CI uses ******2****** as its primary enterprise vulnerability scanning tool. ***2*** uses the Common Vulnerability Scoring System as an evaluating metric in the reports. This scoring system provides an open framework for consistently communicating the characteristics and impacts of information technology vulnerabilities. Its quantitative model ensures repeatable, accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores.

We reviewed two ***2*** vulnerability reports, using **********2**********, for all CI domain controllers in order to evaluate the effectiveness of the CI vulnerability scanning program. The first report, dated December 5, 2017, provided vulnerability ranking of high, medium, or low vulnerability scores for each domain controller. We found that there were no high or critical vulnerabilities on the first report. Specifically, 74 (8 percent) of 981 entries were identified as medium-level risk vulnerabilities, and the report showed no low-level vulnerabilities.

The second report, also dated December 5, 2017, 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 scanning intervals between dates did not exceed two weeks, except in one instance. We found 74 entries with medium risk that were not remediated; however, 70 of those entries were only discovered in the most recent scan.

Along with 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 CI system administrators, using Symantec® Endpoint Protection's management console, to evaluate these requirements for the CI domain controllers and observed on-site 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 we ran the report on-site.

We also reviewed the CI policy for patch management and determined that the policy establishes procedures on how to review, test, approve, and deploy patches. The IRM requires a patch management process for all information systems and procedures to ensure that patches are installed. Because we found no high or critical vulnerabilities reported by the ***2*** scans and the medium-level vulnerabilities were minimal, we did not further investigate CI patch management processes beyond ensuring that proper procedures existed.

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. The IRS made a risk-based decision to continue use of Windows Policy Checker past its end of life in May 2016. That risk-based decision was granted until July 31, 2017. CI continues to report its compliance scores to the Cybersecurity organization.

We reviewed the Windows Policy Checker scans and reports for the CI domain controllers and found that all domain controllers failed, with an average score of 63.76 percent as of August 3, 2017. According to the Windows Policy Checker user manual and Windows Policy Checker reports, scores 79 percent and below are not compliant and present a serious risk to the IRS. We ran a second round of reports on the domain controllers with a CI System Administrator on December 6, 2017, which resulted in the same failing average score of 63.76 percent.

CI personnel told us that they submit their Windows Policy Checker reports monthly to the Cybersecurity organization. We interviewed Cybersecurity officials to determine what further action is taken on failing reports. Cybersecurity personnel collect all Windows Policy Checker reports from various business units, consolidate the information, and then report monthly to the Treasury Cyber Analysis and Reporting Dashboard. We received the Security Assessment Report showing that the IRS is aware of deficiencies with failing CI Windows Policy Checker reports; however, we found no evidence that the Cybersecurity organization provided feedback or guidance to CI data owners of failing systems for the purpose of taking remediation action. By not providing feedback based on CI Windows Policy Checker reports, including how to properly configure system components to the most restrictive settings for failing CI domain controllers, the IRS compromises the security posture of the system. A compromise can lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing and data exploitation, all of which compromise the integrity, confidentiality, and availability of the system.

Furthermore, we found that Windows Policy Checker itself is out of date. The current version of Windows Policy Checker was released December 2014. The Windows Policy Checker uses

Security Technical Implementation Guidelines set by the Defense Information Systems Agency that are over three years old to evaluate IRS systems. By comparison, the most current Security Technical Implementation Guidelines for domain controllers were released October 27, 2017. The IRS cannot provide relevant and timely continuous monitoring with an application so outdated. The IRS will not be able to continuously assess or analyze security controls and security risks to support organizational risk-based decisions by using outdated standards.

Account controls

In accordance with the IRM, information systems shall uniquely identify and authenticate organizational users or processes acting on behalf of organizational users. 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 inactivity in accordance with the IRM policy. The IRM states that the disabling of inactive accounts shall be automated. We determined that CI does not have an automated process for discovering and disabling accounts. According to a CI system administrator, the manual process to review account inactivity is time-consuming, and CI is therefore not complying with policy to determine the period of account inactivity. As a result, CI cannot ensure that inactive accounts are disabled, quarantined, and removed within the appropriate time frames.

We also reviewed CI system settings governing account password and lockout policies and found that they are in compliance with current IRM requirements. However, when we evaluated accounts individually, we found 295 service account exceptions and 1,751 user account exceptions due to improper configurations. Figure 3 shows the total number of service and user account policy exceptions we found in the CI forest.

Figure 3: Summary of Account Policy Exceptions

Policy Exception	Number of Exceptions
Enabled service accounts are located outside the service accounts organizational unit.	7
Enabled service accounts do not follow the proper naming standard.	41
Enabled service account passwords set to not expire.	247
Enabled user accounts using passwords have passwords set to never expire.	25
Enabled user accounts are not required to use PIV card.	1,726

Source: Treasury Inspector General for Tax Administration analysis of information collected from the Users and Computers feature within AD using PowerShell.®

Based on these results, we determined that CI is not effectively enforcing policy governing services and user accounts. Attackers frequently discover and exploit legitimate but inactive user 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 CI's sensitive data at risk for loss, manipulation, and other unauthorized access.

Recommendations

The Chief, CI, with assistance from the Chief Information Officer, should:

Recommendation 6**:** Ensure that business units with failing configuration compliance scores are provided feedback and remediation guidance.

> ***Management's Response:*** The IRS agreed with the recommendation. The IRS Cybersecurity organization plans to provide CI with feedback and remediation guidance to ensure that CI systems with failing configuration compliance scores meet IRS security configuration settings.

Recommendation 7: Ensure that applications used as 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 the recommendation. With support from the Cybersecurity organization, CI plans to transition to the enterprise Continuous Diagnostics and Mitigation security configuration management solution along with up-to-date benchmarks of contemporary secure configuration settings.

Recommendation 8: Review all user accounts in the CI forest and ensure that they are in compliance with IRM policy regarding account disabling, quarantining, and removal and that CI AD architecture is capable of automating the process for discovering and disabling inactive accounts.

> ***Management's Response:*** The IRS agreed with the recommendation. The IRS plans to update its current manual process of disabling user accounts after 120 days of inactivity to an automated process that executes as a scheduled task. In addition, the IRS is drafting a risk-based decision that supports current eDiscovery requirements to not systemically remove any disabled account prior to the completion of employee personnel actions.

Recommendation 9: Ensure that user 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 the recommendation. All users that can be issued PIV cards and have a functional PIV are using the PIV in accordance with IRM 10.8.1.4.7.1.1 whereby any access to network or local resources, including with a privileged account, are required to use multifactor authentication. For those users who do not possess a PIV card (or have one that is temporarily nonfunctional), the IRS is

following the established IRS enterprise exception process. In addition, the IRS stated that it removed all unnecessary test accounts from the production environment and plans to ensure that user accounts are not set to "never expire."

Recommendation 10***:*** Ensure that service account passwords are appropriately configured to expire, follow appropriate naming conventions, and reside in correct organizational units in accordance with policy.

Management's Response: The IRS agreed with this recommendation. The IRS stated that it has appropriately reconfigured all the referenced service accounts. In addition, the IRS plans to work with system owners to rename service account names as directed in IRM 10.8.1.4.1.1.7.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective was to review the IRS ADTAB and evaluate the effectiveness of CI's AD implementation.[1] To accomplish our objective, we:

I. Evaluated the ADTAB's management and oversight for all IRS AD forests.

- A. Conducted research and obtained Federal, Office of Management and Budget, and IRM policies and procedures that govern AD implementation and changes.
- B. Interviewed members of the ADTAB to determine the current duties performed by the members on the board.
- C. Determined whether ADTAB oversight for primary objectives contained within the ADTAB charter are being adequately performed.

II. Evaluated CI's AD forest domain controllers to determine whether they meet minimum baseline security controls established by Federal guidance, IRS policy, Microsoft recommended practices, and industry best practices.

- A. Obtained and evaluated Group Policy Objects for the CI forest and ensured that they properly met criteria. We also obtained and reviewed Group Policy Object reports pertaining to the CI forest.
- B. Obtained a list of CI group, service, and user accounts in AD and ensured that they properly adhered to IRM policies and best practices.
- C. Obtained, reviewed, and evaluated Window Policy Checker outputs for domain controllers in the CI forest.

III. Evaluated physical security policies and procedures at CI's remote sites where domain controllers reside.

- A. Determined necessary criteria to evaluate physical security controls.
- B. Evaluated environmental protections and assessed against relevant criteria.
- C. Evaluated physical access controls and assessed adequacy against relevant criteria.

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

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

A. Reviewed vulnerability scans for CI domain controllers.

B. Determined whether vulnerabilities are being properly remediated.

C. Reviewed antimalware protection on all CI domain controllers.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: NIST requirements for security and privacy of Federal information systems and IRM policies related to physical and environmental security controls. Through interviews with IRS personnel and review of relevant documentation provided by the IRS, we gained an understanding of policies and procedures related to its AD architecture. We examined reports developed from scans using Window Policy Checker application, **********2**********, and Symantec Endpoint Protection's 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 R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
John L. Ledford, Director
Jena Whitley, Audit Manager
Jason McKnight, Lead Auditor
Michael Curtis, Senior Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief, Criminal Investigation
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Enterprise Services
Director, Office of Audit Coordination

Appendix IV

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	Verifying 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.
Change Control	The procedures to ensure that all changes are controlled, including the submission, recording, analysis, decisionmaking, approval, implementation, and post-implementation review of the change.
Cipher Lock	Makes use of a feature keypad in place of standard keyhole. This type of lock provides easy access to any building by the use of a numerical pin code in place of a key.
Common Vulnerability Scoring System	Provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities.
Computer Operations Administrator	CI personnel responsible for providing desktop and systems administration support to customers within a business unit. Duties include supporting wireless technology, networking, software applications, hardware platforms, and peripheral devices.
Criminal Investigation	An IRS business unit that serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law.

Term	Definition
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.
Enterprise Computing Center	Supports tax processing and information management through a data processing and telecommunications infrastructure.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Forest	A complete instance of AD. Each forest acts as a top-level container in that it houses all domain containers for that particular AD instance.
Group Policy Object	A virtual collection of policy settings.
Integrated Submission and Remittance Processing	A System that transcribes and formats data from paper returns, documents, and vouchers for input into the Generalized Mainline Framework and other systems by key entry operators. It also captures check images for archiving.
Limited Area	An area in a building to which 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 Facilities Management and Security Services Physical Security Section Chief based on critical assets.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have 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.

Term	Definition
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
Patches	An update to an operating system, application, or other software issued specifically to correct particular problems with the software.
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	PowerShell is an automated task framework from Microsoft, with a command line shell and a scripting language integrated into the .NET framework, which can be embedded within other applications.
Scalable	Capable of being easily expanded or upgraded on demand.
Security Assessment Report	Provides the stakeholders with an assessment of the adequacy of the security and privacy controls used to protect the confidentiality, integrity, and availability of the system and the data it stores, transmits, or processes.
Security Technical Implementation Guides	Configuration standards for Department of Defense Information Assurance and Information Assurance enabled devices/systems. They contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.
Steering Committee	A committee that decides on the priorities or order of business of an organization and manages the general course of its operations.
Symantec Endpoint Protection	Symantec Endpoint Protection is a client-server solution that protects laptops, desktops, and servers in your network against malware, risks, and vulnerabilities.

Term	Definition
Treasury Cyber Analysis and Reporting Dashboard	A product of the Treasury's Cyber Security Dashboard which provides an executive overview of the Treasury Department's security posture to its stakeholders. The Cyber Security Dashboard aggregates security data from bureaus and other sources to provide a current snapshot of the Treasury Department's information security status in order to identify emerging trends and respond to potential threats.
*******2*******	**********2********** ********2*******.
*******2******* *******2*******	**********2**********.
Trusts	A relationship established between domains that makes it possible for users in one domain to be authenticated by a domain controller in the other domain.
Two-Factor Authentication	A method of confirming a user's claimed identity by using a combination of two different components. These components may be something that the user knows, something that the user possesses, or something that is inseparable from the user.
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 V

Management's Response to the Draft Report

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

Criminal Investigation

May 16, 2018

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: J. Don Fort
Chief, Criminal Investigation

S. Gina Garza
Chief Information Officer

SUBJECT: Response to Draft Report – Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls (Audit # 201720019)

Thank you for the opportunity to review and comment on the draft report. Attached is a detailed response outlining our corrective actions.

We agree with your recommendations and Criminal Investigations (CI), Information Technology, and Facilities Management will collaborate on the recommended corrective actions. These include ensuring that: (1) the Active Directory Technical Advisory Board is providing agency-wide oversight and updating its charter; (2) CI computer rooms comply with IRM requirements and meet Federal and internal security standards; (3) local personnel are properly trained;(4) compliance checker applications use up-to-date guidelines; (5) Active Directory user accounts are in compliance with internal policy; and (6) ensure user accounts and service accounts are appropriately configured.

Approximately 60% of the physical security weaknesses identified can be addressed by updating signage, badge designation, and limited area access lists.

If you have any questions, please contact Chief Don Fort or Deputy Chief Eric Hylton in the Criminal Investigation office at (202) 317-3200.

Attachment

Attachment

Our comments on the specific recommendations in this report are as follows:

RECOMMENDATION #1: The Chief Information Officer should review the current scope of the ADTAB's defined oversight responsibilities and modify as necessary to ensure that the ADTAB is providing agency-wide oversight of the AD architecture, including the AD forests that operate outside of the Enterprise Operations organization.

CORRECTIVE ACTION #1: IRS agrees with this recommendation and will review the current scope of the Active Directory Technical Advisory Board's (ADTAB's) defined oversight responsibilities and modify as necessary.

IMPLEMENTATION DATE: June 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Information Officers for Enterprise Operations and Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We will monitor this corrective action as a part of our internal management control system.

RECOMMENDATION #2: The Chief Information Officer should update the existing ADTAB charter and ensure that all individual owners are appropriately represented on the ADTAB

CORRECTIVE ACTION #2: IRS agrees with this recommendation and will update the existing ADTAB charter and ensure that all individual owners are appropriately represented on the ADTAB.

IMPLEMENTATION DATE: June 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Information Officers for Enterprise Operations and Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We will monitor this corrective action as a part of our internal management control system.

RECOMMENDATION 3: The Chief, Criminal Investigation, with assistance from the Chief Information Officer, should complete a cost analysis to determine the efficacy of relocating CI assets in each of the field offices to existing IRS computer rooms versus upgrading the CI computer rooms to ensure assets are protected in accordance with Federal and IRM security requirements, and implement the most cost effective solution.

PROPOSED MANAGEMENT RESPONSE: The IRS agrees with this recommendation. Specifically, CI will collaborate with the Facilities Management and Security Services (FMSS) and Information Technology divisions to complete a joint analysis of each

computer room in CI field offices within 12 months and determine the most effective and efficient course of action to meet Federal and IRM security standards. The joint analysis will address the technological, operational, physical location, funding and time factors necessary to either relocate the assets to existing IRS computer room(s) or bring the computer room(s) into compliance. The joint cost analysis will then be the basis for a developing joint project plan to implement the proposed solutions contingent with the time needed to properly plan and fund either the relocation of CI assets or secure those assets in the existing locations.

IMPLEMENTATION DATE: Cost-Benefit Analysis by July 15, 2019. Implementation date determined by cost-benefit analysis.

RESPONSIBLE OFFICIALS: Director Technology Operations and Investigative Services (TOIS) and Associate Chief Information Officers for Enterprise Operations and Enterprise Services.

Recommendation 4: The Chief, Criminal Investigation, with assistance from the Chief Information Officer, should ensure that CI computer rooms are immediately updated to comply with IRM requirements for limited areas, key and cipher lock combination controls, and standalone fire extinguishers while a cost effective solution regarding the computer room location is identified and implemented.

PROPOSED MANAGEMENT RESPONSE: The IRS agrees with this recommendation. Specifically, CI will partner with FMSS to identify the steps needed to comply with Limited Area access controls, safeguard keys and lock combinations, and requirements for standalone fire extinguishers in CI computer room locations, and develop within 12 months a joint project plan to address these IRM requirements.

IMPLEMENTATION DATE: July 15, 2019

RESPONSIBLE OFFICIALS: Director Technology Operations and Investigative Services (TOIS) and Associate Chief Information Officers for Enterprise Operations and Enterprise Services.

RECOMMENDATION #5: The Chief, Criminal Investigation, with assistance from the Chief Information Officer, should ensure that local Computer Operations Administrator personnel are properly trained to understand and comply with IRS policies and procedures governing Limited Areas and provide oversight to ensure that these policies and procedures are kept current.

CORRECTIVE ACTION #5: The IRS agrees with the recommendation. Specifically, CI will conduct training for all Computer Operations Administrator personnel on IRS policies and procedures governing Limited Areas and will ensure these policies and procedures are followed.

IMPLEMENTATION DATE: October 15, 2018

RESPONSIBLE OFFICIALS: Director Technology Operations and Investigative Services (TOIS)

CORRECTIVE ACTION MONITORING PLAN: We will monitor this corrective action as a part of our internal management control system.

RECOMMENDATION #6: The Chief, Criminal Investigation, with assistance from the Chief Information Officer, should ensure that business units with failing configuration compliance scores are provided feedback and remediation guidance.

CORRECTIVE ACTION #6: We agree with the recommendation. Cybersecurity will provide CI with feedback and remediation guidance to ensure CI systems with failing configuration compliance scores meet IRS security configuration settings.

IMPLEMENTATION DATE: October 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We will monitor this corrective action as a part of our internal management control system.

RECOMMENDATION #7: The Chief, Criminal Investigation, with assistance from the Chief Information Officer, should ensure that applications used as compliance checkers use up-to-date guidelines to provide recognized, standardized, and established benchmarks that stipulate contemporary secure configuration settings.

CORRECTIVE ACTION #7: We agree with the recommendation. Criminal Investigation with support from IT Cybersecurity will transition to the enterprise Continuous Diagnostics and Mitigation (CDM) security configuration management solution along with up to date benchmarks of contemporary secure configuration settings.

IMPLEMENTATION DATE: October 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We will monitor this corrective action as a part of our internal management control system.

RECOMMENDATION #8: The Chief, Criminal Investigation, with assistance from the Chief Information Officer, should ensure review all user accounts in the CI forest and ensure that they are in compliance with IRM policy regarding account disabling, quarantining, and removal and that CI AD architecture is capable of automating the process for discovering and disabling inactive accounts.

CORRECTIVE ACTION #8: We agree with the recommendation. IRS/CI will update its current process of the manual process of disabling user accounts after 120 days of inactivity to an automated process which executes as a scheduled task. In addition, IRS/CI is drafting a Risk Based Decision (RBD) that supports current eDiscovery requirements to not systemically remove any disabled account prior to the completion of employee departure retention actions.

IMPLEMENTATION DATE: December 15, 2018

RESPONSIBLE OFFICIALS: Director Technology Operations and Investigative Services (TOIS)

CORRECTIVE ACTION MONITORING PLAN: We will monitor this corrective action as a part of our internal management control system.

RECOMMENDATION #9: The Chief, Criminal Investigation, with assistance from the Chief Information Officer, should ensure that user account passwords are appropriately configured to expire and require that PIV cards be used in accordance with policy.

CORRECTIVE ACTION #9: We agree with the recommendation. All users that can be issued Personal Identity Verification (PIV) cards and have a functional PIV are using the PIV in accordance with IRM10.8.1.4.7.1.1 whereby any access to network or local resources, including with a privileged account, are required to use multifactor authentication. For those users who do not possess a PIV card (or have one that is temporarily non-functional) we are following the established IRS enterprise exception process. In addition, we have removed all unnecessary test accounts from production environment and will ensure user accounts are not set to "never expire".

IMPLEMENTATION DATE: December 15, 2018

RESPONSIBLE OFFICIALS: Director Technology Operations and Investigative Services (TOIS)

CORRECTIVE ACTION MONITORING PLAN: We will monitor this corrective action as a part of our internal management control system.

RECOMMENDATION #10: The Chief, Criminal Investigation, with assistance from the Chief Information Officer, should ensure that service accounts are appropriately configured to expire, follow appropriate naming conventions, and reside in correct organizational units in accordance with policy.

CORRECTIVE ACTION #10: We agree with this recommendation; IRS/CI has appropriately re-configured all the referenced service accounts. In addition, IRS/CI will work with system owners to rename service account names as directed in IRM 10.8.1.4.1.1.7.

IMPLEMENTATION DATE: December 15, 2018

RESPONSIBLE OFFICIALS: Director Technology Operations and Investigative Services (TOIS)

CORRECTIVE ACTION MONITORING PLAN: We will monitor this corrective action as a part of our internal management control system.