Inadequate Management of Active Directory Puts USPTO's Mission at Significant Cyber Risk

FINAL REPORT NO. OIG-19-014-A

JUNE 13, 2019

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

JUNE 13, 2019

MEMORANDUM FOR: Andrei Iancu
Under Secretary of Commerce for Intellectual Property
and Director of the U.S. Patent and Trademark Office

FROM: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *Inadequate Management of Active Directory Puts USPTO's Mission at Significant Cyber Risk*
Final Report No. OIG-19-014-A

Attached is our final audit report regarding USPTO's Active Directory. Our objective was to determine whether USPTO has adequately managed its Active Directory to protect mission critical systems and data.

We found that USPTO (1) inadequately managed its Active Directory, and (2) poorly protected its critical IT assets hosting Active Directory. These deficiencies put the USPTO mission at significant cyber risk. Regarding USPTO inadequately managing its Active Directory, we found that inadequate configuration of Active Directory allowed excessive access permissions; user credentials were not securely stored in Active Directory; weak passwords were used; and a security best practice was not followed to enforce multi-factor authentication. Regarding USPTO poorly protecting its critical IT assets hosting Active Directory, we found that vulnerability scanning practices were inadequate to identify and remediate vulnerabilities; no baseline existed for authorized ports and services; and critical vulnerabilities were not remediated in a timely manner. USPTO immediately began to take action during our audit to remediate some of these security deficiencies. However, we remain concerned with USPTO's commitment to prioritizing improvement of its security posture. We identified, in finding 2, the same security deficiencies that we reported 2 years ago, specifically relating to vulnerability scanning and port management.

On May 16, 2019, we received USPTO's response to the draft report's findings and recommendations, which we include within the report as appendix C. USPTO concurred with all recommendations, noting that USPTO is currently taking actions to address each recommendation.

Pursuant to Department Administrative Order 213-5, please submit to us an action plan that addresses the recommendations in this report within 60 calendar days. The final report will be posted on OIG's website pursuant to sections 4 and 8M of the Inspector General Act of 1978, as amended (5 U.S.C. App., §§ 4 & 8M).

We appreciate the cooperation and courtesies extended to us by your staff during this audit. If you have any questions or concerns about this report, please contact me at (202) 482-1931 or Dr. Ping Sun, Director for IT Security, at (202) 482-6121.

cc: Terryne Murphy, Acting Chief Information Officer
Henry "Jamie" Holcombe, Chief Information Officer, USPTO
Welton Lloyd, Audit Liaison, USPTO
Maria Stanton-Dumas, IT Security Audit Action Officer
Joselyn Bingham, Audit Liaison, Office of the Chief Information Officer
MaryAnn Mausser, Audit Liaison, Office of the Secretary

Report in Brief

JUNE 13, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

Inadequate Management of Active Directory Puts USPTO's Mission at Significant Cyber Risk

OIG-19-014-A

Background

The Department of Commerce and its bureaus are required to follow federal laws to secure information technology (IT) systems through the cost-effective use of managerial, operational and technical controls.

This responsibility applies to all IT systems, including U.S. Patent and Trademark Office (USPTO) systems. The agency heavily relies on IT infrastructure to support its mission–critical systems and applications.

One critical component of USPTO IT infrastructure is Active Directory, which maintains a logical structure, known as a domain, for USPTO to manage all network resources within the domain.

Due to the nature of its role, Active Directory holds sensitive information such as users' credentials and network topologies, making it a prime target for cyberattacks. USPTO must ensure adequate security of its Active Directory to avoid complete compromise of its network.

Why We Did This Review

Our audit objective was to determine whether USPTO has adequately managed its Active Directory to protect mission critical systems and data.

Our review focused on fundamental security practices of Active Directory management and security control implementations of the servers hosting Active Directory.

WHAT WE FOUND

We found that USPTO (1) inadequately managed its Active Directory, and (2) poorly protected its critical IT assets hosting Active Directory. These deficiencies put the USPTO's ability to accomplish its mission at significant risk. Regarding USPTO inadequately managing its Active Directory, we found that:

1. inadequate configuration of Active Directory allowed excessive access permissions;
2. user credentials were not securely stored in Active Directory;
3. weak passwords were used; and
4. a security best practice was not followed to enforce multi-factor authentication.

Regarding USPTO poorly protecting its critical IT assets hosting Active Directory, we found that:

1. vulnerability scanning practices were inadequate to identify and remediate vulnerabilities;
2. no baseline existed for authorized ports and services; and
3. critical vulnerabilities were not remediated in a timely manner.

USPTO immediately began to take action during our audit to remediate some of the security deficiencies. However, we remain concerned with USPTO's commitment to prioritizing improvement of its security posture. We identified, in finding 2, the same security practice deficiencies that we identified and reported 2 years ago, specifically relating to vulnerability scanning and port management.

WHAT WE RECOMMEND

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office direct the Chief Information Officer to take the following actions:

1. Immediately (1) reevaluate the current Active Directory configuration based on users' roles and responsibilities, (2) reorganize Active Directory user groups based on job functions, and (3) remove any unneeded privileges.
2. Eliminate weak credential encryption to the maximum extent possible. For those applications that currently do not support strong encryption, implement additional compensating controls to protect credentials.
3. Ensure that all passwords meet the standards set by Department and USPTO policies or implement additional compensating controls to protect them. Furthermore, consider incorporating a password policy that emphasizes password length, a primary factor in characterizing password strength recommended by NIST guidelines.
4. Ensure PIV card technology compatibility with on-going and future system development for USPTO next-generation applications, and switch PIV enforcement to a per-user basis, when technically feasible.
5. Finalize the vulnerability-scanning SOP and ensure it includes requirements to verify scanning tools are updated prior to scans and credentialed scanning is performed on physical and virtual machines.
6. Apply the principle of least functionality by developing an authorized open port baseline for system operation, enforce it, and establish an approval procedure for open port requests that deviate from the baseline.
7. Work with USPTO contracting officers to ensure effective government oversight of contractors performing vulnerability assessment scans.
8. Streamline the patch management change-review policies and procedures to allow for timely vulnerability remediation.

Contents

Introduction

The Department of Commerce and its bureaus are required to follow federal laws to secure information technology (IT) systems[1] through the cost-effective use of managerial, operational and technical controls. This responsibility applies to all IT systems, including U.S. Patent and Trademark Office (USPTO) systems.

USPTO's mission is to foster innovation, competitiveness, and economic growth—domestically and abroad—by delivering high quality and timely examination of patent and trademark applications. The agency heavily relies on IT infrastructure to support its mission–critical systems and applications.

One critical component of USPTO IT infrastructure is Active Directory, which maintains a logical structure, known as a domain,[2] for USPTO to manage all network resources within the domain. If deployed and managed properly, Active Directory can provide USPTO a securely centralized means to manage network users, workstations, servers, printers, databases, and system configuration as illustrated in figure 1. Due to the nature of its role, Active Directory holds sensitive information such as users' credentials and network topologies, making it a prime target for cyberattacks. USPTO must ensure adequate security of its Active Directory to avoid complete compromise of its network.

Figure 1. The Concept of Active Directory

Source: OIG

[1] See Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551, et seq.

[2] A domain is simply a networked group of users, workstations, servers, printers, software applications (e.g., databases and websites) as well as other network devices. Everything within the domain is controlled by Active Directory.

Objective, Findings, and Recommendations

Our audit objective was to determine whether USPTO has adequately managed its Active Directory to protect mission critical systems and data. See appendix A for further details regarding our objective, scope, and methodology. Our review focused on fundamental security practices of Active Directory management and security control implementations of the servers hosting Active Directory.

We found that USPTO (1) inadequately managed its Active Directory, and (2) poorly protected its critical IT assets hosting Active Directory. These deficiencies put the USPTO's ability to accomplish its mission at significant risk. Regarding USPTO inadequately managing its Active Directory, we found that:

- inadequate configuration of Active Directory allowed excessive access permissions;
- user credentials were not securely stored in Active Directory;
- weak passwords were used; and
- a security best practice was not followed to enforce multi-factor authentication.

Regarding USPTO poorly protecting its critical IT assets hosting Active Directory, we found that:

- vulnerability scanning practices were inadequate to identify and remediate vulnerabilities;
- no baseline existed for authorized ports and services; and
- critical vulnerabilities were not remediated in a timely manner.

USPTO immediately began to take action during our audit to remediate some of the security deficiencies. However, we remain concerned with USPTO's commitment to prioritizing improvement of its security posture. We identified, in finding 2, the same security practice deficiencies that we identified and reported 2 years ago, specifically relating to vulnerability scanning and port management.[3]

I. USPTO Inadequately Managed Its Active Directory

Active Directory plays a critical role in securing USPTO networks. It stores usernames and passwords of all users as well as enforces multi-factor authentication.[4] We analyzed Active Directory data and found that it was inadequately managed. Specifically, (1) an inadequate configuration of Active Directory allowed excessive access permissions, (2) user credentials

[3] Department of Commerce Office of Inspector General, March 24, 2017. *Inadequate Security Practices, Including Impaired Security of Cloud Services, Undermine USPTO's IT Security Posture*. OIG-17-021-A. Washington, DC: DOC OIG.

[4] Multi-factor authentication provides additional security beyond traditional username/password authentication because it requires that more than one authentication method is used—such as a combination of password, token (i.e., a hardware device used for authentication, such as an identification card or key fob), fingerprint, or other means.

were not securely stored in Active Directory, (3) weak passwords were used, and (4) a security best practice was not followed to enforce multi-factor authentication.

A. Inadequate configuration of Active Directory allowed excessive access permissions

One of the primary tasks in Active Directory is to manage user accounts' access permissions. To facilitate this management, Active Directory user accounts are usually combined into separate groups with varying permission levels. To comply with the least privilege security principle, a National Institute of Standards and Technology (NIST) control requirement,[5] each group must be given access permissions only to relevant function areas required by users' roles and responsibilities. For example, all users responsible for managing network printers should be placed in a group that only has needed access privileges for them to be able to fulfill this task.

We found that USPTO did not adequately separate the users into groups based on their job functions, resulting in granting excessive access privileges to users. For example, USPTO created a privileged group with highly elevated privileges. This group has a wide range of permissions from managing user accounts to managing system backup, network printing, and server operation**.** Even though many of its members only needed permission to perform system backups or other operation tasks, the group permissions allowed any member to create, modify, and delete user accounts, or access sensitive information, such as other users' credentials (usernames and passwords). The fundamental security principle of least privilege[6] would require separating users into groups with appropriate permissions based on job roles. However, USPTO put many users who performed different tasks (e.g. managing servers, printers, or accounts) into this privileged group to satisfy operation needs. As a result, users were granted excessive access privileges that were not needed to perform their job functions. As a result of this finding, USPTO is currently reviewing the group to separate its users based on their job functions.

USPTO did not follow the least privilege principle to restrict users' permissions to only what is necessary for their job functions. According to USPTO officials, this happened because the users and groups in Active Directory were not properly organized based on their functionalities when it was deployed in 2002. Over the subsequent16-year period, Active Directory was upgraded several times but user group structure was never thoroughly reexamined. Moreover, Active Directory was rather complex, which, at the time we started this audit, encompassed more than 260,000 objects (e.g., users, groups, and servers) that have to be managed. As a result, Active Directory configuration was often performed simply by following the inherited practices from the past, such as conveniently adding a user into the privileged group even if the user did not need all the elevated privileges.

In addition, USPTO did not adequately review and remove access permissions for users who no longer needed them, because it did not have an established process for reviewing

[5] National Institute of Standards and Technology, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53, Rev 4. Gaithersburg, MD: NIST.

[6] Ibid, Control AC-6, Least Privilege.

accounts and removing unnecessary permissions. We found that at least 19 out of 241 users did not have any business need to be granted escalated permissions, including access to all Active Directory users' credentials. Although USPTO took action and removed these 19 user accounts once they were identified, prior to that time certain users were not prevented from having access to information resources that were no longer required for performing their jobs. This presents a great risk to USPTO, as more users having special access privileges increases the risk of compromise. Compromise with escalated privileges can lead to the disclosure of sensitive information, such as other users' usernames and passwords, especially when numerous users' passwords were not securely stored in Active Directory.

B. *User credentials were not securely stored in Active Directory*

Because Active Directory is used to centrally authenticate domain users on the network, it stores users' credentials (usernames and passwords) in its database. Such highly sensitive information should be stored using strong encryption. The Department password management policy requires that "[p]asswords must not be stored electronically in clear text or in any easily deciphered form."[7] We found that USPTO did not configure Active Directory correctly, resulting in more than 200 user account passwords being insecurely stored, which violated the Department policy. Although this may seem like a small percentage in relation to a total number of approximately 30,000 Active Directory user accounts, it does not diminish the risk. Each insecurely stored password can provide an opportunity for attackers to compromise the USPTO IT systems and information. Specifically:

- *37 accounts had passwords stored using particularly weak encryption.* This allowed us to obtain passwords instantly, one of which was a privileged account controlling email servers.

- *166 accounts had passwords stored using insecure encryption.* Using freely available software and a laptop with average computing power, we were able to crack passwords for 79 accounts within approximately 50 minutes. Two of the accounts were privileged accounts allowing access to all domain users' credentials.

During the authentication process, user credentials, including passwords, are transmitted across the network to authenticate users or systems when requesting access to network resources. Currently, there are various hacking tools available to help an attacker intercept the transmitted credentials or retrieve them from the servers hosting Active Directory. In addition, with certain access privilege, some user accounts can directly access Active Directory-encrypted credentials. Once such a privileged account has been compromised, the attacker can easily make a copy of the credentials, and perform offline

[7] DOC, September 21, 2012. *Password Management, Commerce Information Technology Requirement 021* (CITR-021). Washington, DC: DOC, 3(7.2).

password cracking, which can greatly increase the success rate of cracked passwords. As a result, using strong encryption is vital to protect user credentials and reduce the risk of compromise.

According to USPTO officials, the reason for not adopting strong encryption was largely related to USPTO legacy systems, which may not be compatible with newer encryption technology. To ensure the legacy systems' operation, USPTO leaves the weak encryption configurations untouched until the systems are replaced. Currently, USPTO plans to replace its legacy systems by 2022. Until then, these weak encrypted credentials will continue to present a significant security risk to the USPTO mission.

C. Weak passwords were used

The risk associated with weak Active Directory encryption can be somewhat mitigated by users using long and complex passwords,[8] making it harder for an attacker to crack (and resulting in better protection of sensitive information assets). Strong, complex passwords—which are required by Department password management policy[9]—must be of sufficient length and contain a mixture of upper and lower case letters, numbers, and special characters.

After cracking the weak encryption of 116 passwords, we reviewed and found that almost all (112, or 97 percent) did not comply with the Departmental password policy. These weak passwords made it considerably easier for an attacker to successfully employ brute-force attacks[10] and gain unauthorized access. The use of long and complex passwords has been a long-standing security practice for several decades. Nevertheless, USPTO failed to achieve this fundamental security practice. In 2015, USPTO implemented a password policy enforcement tool to ensure that the newly created passwords comply with the Departmental requirement. However, the majority of these weak passwords were associated with accounts used by its legacy systems, which were deployed prior to the tool implementation. USPTO's inaction of updating these weak passwords left the legacy systems very susceptible to cyberattack.

[8] NIST, June 2017. *Digital Identity Guidelines: Authentication and Lifecycle Management*, NIST SP 800-63B. Gaithersburg, MD: NIST, Appendix A.

[9] *See* CITR-021.

[10] A brute-force attack is characterized by repeated attempts to gain access to a system by presenting all possible combinations of access credentials, such as passwords, until a match is found.

D. A security best practice was not followed to enforce multi-factor authentication

Active Directory allows users to use Personal Identity Verification (PIV) cards for multi-factor authentication, and can enforce such authentication by preventing users from logging into the network using passwords. PIV authentication is a federal requirement[11] and USPTO has deployed PIV cards for its users to be in compliance. However, we found that USPTO chose not to use the most secure way to enforce PIV authentication. Specifically, USPTO configured its Active Directory to enforce PIV card authentication on a per-computer basis. This method is less secure because users still have their passwords stored in Active Directory, which could provide an opportunity for an attacker to obtain and use them to compromise USPTO information systems. The impact of the less secure configuration is compounded in this case by the use of weak passwords.

The best practice[12] is to enforce multi-factor authentication on a per-user basis. This way all user passwords would be replaced in Active Directory with an encrypted string[13] of 120 characters, which makes compromise significantly more difficult. However, authentication on a per-user basis is currently not attainable at USPTO, as some of the USPTO legacy systems do no support PIV cards.

II. USPTO Poorly Protected Its Critical IT Assets Hosting Active Directory

USPTO deploys 12 domain controllers to support its Active Directory function. A domain controller is a Windows server that acts as the gatekeeper to the domain. It provides a central location for administrators to manage Active Directory and enforce policies and procedures. Having access to a domain controller can be considered possessing "the keys to the kingdom" because of the inherent elevated privilege and near absolute authority over IT infrastructure.

We reviewed fundamental security controls on these 12 domain controllers, as well as 41 supporting hypervisors,[14] and found that USPTO's vulnerability scanning practices were inadequate. We also found an excessive number of authorized ports and unnecessarily open ports on domain controllers that increase the security risk of USPTO IT infrastructure. In addition, critical vulnerabilities were not remediated in a timely manner.

---

[11] Office of Management and Budget, February 3, 2011. Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*. Washington, DC: OMB.

[12] Esquivel, Jesse. "Smart Card Logon Enforcement—Long Edition!" Microsoft.com. [online] https://blogs.technet.microsoft.com/nextnextfinish/2017/09/15/smart-card-logon-enforcement-long-edition/ (accessed October 1, 2018).

[13] A string is simply a sequence of characters that may include letters, numbers, or special characters.

[14] A hypervisor is a physical server that maximizes hardware efficiency by hosting multiple virtual machines that leverage resource sharing. The USPTO implementation has 9 of the 12 domain controllers utilizing virtualization.

A. *Vulnerability scanning practices were inadequate to identify and remediate vulnerabilities*

Vulnerabilities are weaknesses in a system that may be leveraged by malicious actors to adversely affect the confidentiality, integrity, or availability of the system or information therein. There are many publicly known vulnerabilities related to IT systems generally. In fact, hundreds, if not thousands, of new vulnerabilities are discovered each month. For more information on the trend of vulnerability discovery, see appendix B.

Vulnerability scanning can help identify and correct security weaknesses, through system upgrades or patches, before they can be exploited. Vulnerability scanning helps identify outdated software versions, missing patches, and misconfigurations.

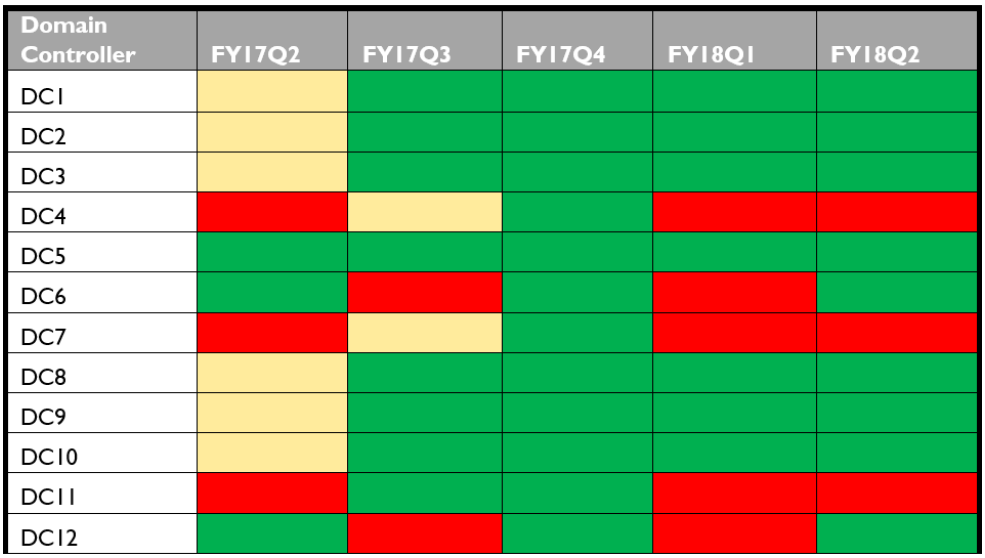
Any time a computer is connected to a network, it is at risk of vulnerability exploitation. Departmental policy therefore requires that bureaus scan all network addressable devices, such as servers and workstations, at least quarterly.[15] Given the high number of vulnerabilities discovered each month, as illustrated in appendix B, performing scans as frequently as possible can assist in timely identification of any known vulnerabilities.

Domain controllers' vulnerability scanning reports of the most recent 5 quarters at the time of our audit (second quarter of fiscal year (FY) 2017 through the second quarter of FY 2018) showed that USPTO did not consistently scan its domain controllers. In fact, only 1 domain controller was scanned each quarter as required. Figure 2 below illustrates our findings of domain controllers scanning practices using the following color-coding:

- *Green* indicates that scanning was performed as required.
- *Yellow* indicates that scans were completed using an outdated scanning tool that cannot identify newly discovered vulnerabilities. (For example: in the second quarter of FY 2017, USPTO scanned 6 domain controllers with a tool that had not been updated since June 2016. Given that thousands of new vulnerabilities can be discovered monthly, and vulnerabilities are becoming more pervasive, scanning tools must be kept up to date to remain effective.)
- *Red* indicates no scans were performed.

[15] DOC, January 25, 2012. *Commerce Information Technology Requirement, Vulnerability Scanning and Patch Management* 016 (CITR-016). Washington, DC: DOC, 6(B).

Figure 2. Domain Controller Quarterly Vulnerability Scanning Practices



Source: OIG analysis

We also found poor scanning practices for domain controller-supporting hypervisors, with only 1 out of 41 undergoing scans, conducted in only 3 out of the 5 quarters. In addition, the vulnerability scans that were conducted on the single hypervisor were not credentialed,[16] which was a violation of Departmental policy[17] and produced far less accurate and informative scanning results. Vulnerability scanning of hypervisors and hosted virtual machines are of equal importance. If a hypervisor is compromised, all hosted virtual machines are considered compromised too.

These deficient scanning practices are the result of two shortcomings: (1) USPTO did not have a formal, documented standard operating procedure (SOP) for performing and managing scans, and (2) there was a lack of government contractor oversight.

Managing the vulnerability scanning process—generally done by contractors in USPTO's Cybersecurity Division—includes updating the system inventory and scanning tool, performing scans, reviewing the scanning results, and sharing vulnerability information with other USPTO groups. According to USPTO, an established informal process does exist, but contractors do not always follow it. The failure to follow established scanning procedures illustrated inadequate government oversight by the Cybersecurity Division, which is charged specifically with overseeing the vulnerability scanning processes and procedures. USPTO took immediate action and began developing a written formal SOP for the vulnerability scanning process after we brought this to their attention. Also, we

[16] There are two options when performing vulnerability scans: credentialed and non-credentialed. Credentialed scans are the better option as they can be configured to have administrative access to the system, which provides for robust scanning reports consisting of more useful and accurate information. Non-credentialed scans, on the other hand, have no access to the system and provide limited information with less accuracy.

[17] Credentialed scans are required per CITR-016, § 6(E).

recognize that the Cybersecurity Division is not the exclusive overseer of contractor performance, and coordination with the USPTO contracting office is crucial to ensure adequate performance of contractors.

B. *No baseline existed for authorized ports and services*

Ports are communication entryways into a system component for network services. When a network service is waiting to accept connections, also known as "listening" on a computer's port, the port is considered open. There are a total of 65,536 ports[18] that services can utilize, but the number of ports required to be open depends upon the system and which services it requires. For example, the Microsoft Windows Server system utilizes only 64 TCP ports to implement its basic functionality.[19]

Ports that are required to be open for a system's functionality should be maintained in the system's security documentation, which acts as a baseline used to authorize the system and support continuous monitoring. Any undocumented ports are considered unauthorized. Documenting and implementing a specific set of permissible ports enforces the principle of least functionality and ensures that an information system is configured to provide only its essential capabilities. This practice can dramatically reduce the attack surface of an information system, thereby reducing the overall risk of operating the system.

We found that USPTO did not document and authorize only the specific ports and services that were needed for the domain controllers' functionality. Rather, USPTO improperly documented every available port, 65,536 in total, and therefore authorized them to be open. Of greater concern, when we questioned actual open ports that are not generally used for Active Directory services, USPTO confirmed that 14 unneeded ports were indeed open on 7 of the 12 domain controllers**.** These unneeded open ports are characteristic of potential malicious activity and could provide attack avenues into Active Directory.

Federal agencies are required to adhere to NIST-defined security control requirements,[20] which include documenting ports and services that are necessary for operations.[21] As mentioned above, this documentation helps system personnel disable all unneeded ports and services, limiting information systems to the least functionality necessary. Because specific ports and running services were not documented, USPTO was unable to properly limit functionality—as demonstrated by having unnecessary ports open on several domain controllers, which significantly increased the risk of potential cyberattack.

USPTO maintains security information for each of its systems in system security plans (SSPs), including authorized open ports and security controls needed for each system. The

[18] These ports are referred to Transmission Control Protocol (TCP) ports only.

[19] Microsoft. *Service Overview and Network Port Requirements for Windows* [online] https://support.microsoft.com/en-us/help/832017/service-overview-and-network-port-requirements-for-windows (accessed on August 30, 2018).

[20] NIST, March 2006. FIPS Publication 200*, Minimum Security Requirements for Federal Information and Information Systems*, NIST SP 800-26. Gaithersburg, MD: NIST, Section 4.

[21] NIST SP 800-53, Rev 4, Control CM-7, Least Functionality.

Cybersecurity Division is responsible for creating and updating SSPs for system owners. Currently, it is the system owners' responsibility to provide accurate information of their systems, so that the SSPs can accurately represent the systems' baselines for security control implementation. While putting collected information into the SSPs, the Cybersecurity Division should validate the given information to ensure compliance with security requirements. For example, when documenting all 65,536 ports in the SSP, the division should have questioned the system owner's response about why these ports were needed on the domain controllers—the most critical components on the USPTO network. According to Cybersecurity Division officials, USPTO did not have documented initial authorized port requirements for various software products such as Windows or Linux operating systems. When we brought this security weakness to its attention, USPTO took action and updated its security documentation to reflect only essential ports and closed the unnecessary ports on domain controllers.

C. Critical vulnerabilities were not remediated in a timely manner

Departmental policy requires that bureaus remediate identified vulnerabilities in a timely manner, depending on the risk impact of the systems as defined by Federal Information Processing Standards (FIPS) 199. Specifically, vulnerabilities must be remediated within 30 days for high-impact systems, 60 days for moderate-impact systems, and 90 days for low-impact systems.[22] Domain controllers are components of the Enterprise Software System (ESS), which carries a moderate-impact rating. Therefore, any vulnerabilities discovered within the system should be remediated within 60 days.

We found that USPTO did not remediate vulnerabilities, including high- and critical-risk vulnerabilities, through timely standard server patching. For example, a high-risk vulnerability, which could allow an attacker to execute malicious code remotely, remained un-remediated for 3 quarters. This happened partly because USPTO has a cumbersome process for testing patches prior to deploying them to production: each patch was required to be tested in multiple lab environments and then endured a change review process, including approval from all applicable owners of the systems that rely on Active Directory authentication, before it was implemented.

By not patching vulnerabilities on the servers in a timely manner, USPTO left its domain controllers vulnerable to potential cyberattacks, thus undermining its entire IT infrastructure.

Having assessed USPTO's fundamental security practices of Active Directory management and security control implementations of the servers hosting Active Directory, we found recurring security practice weaknesses noted previously in our March 2017 audit report.[23] In that earlier report, we specifically pointed out the security weaknesses relating to vulnerability scanning and port management, and made recommendations for USPTO to take corrective actions. However, we have now observed that the same inadequate security practices still exist at USPTO—especially with domain controllers, which are its most critical IT components.

[22] CITR-016, § 6(F)(1).

[23] *See* OIG-17-021-A.

Recommendations

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office direct the Chief Information Officer to take the following actions:

1. Immediately (1) reevaluate the current Active Directory configuration based on users' roles and responsibilities, (2) reorganize Active Directory user groups based on job functions, and (3) remove any unneeded privileges.
2. Eliminate weak credential encryption to the maximum extent possible. For those applications that currently do not support strong encryption, implement additional compensating controls to protect credentials.
3. Ensure that all passwords meet the standards set by Department and USPTO policies or implement additional compensating controls to protect them. Furthermore, consider incorporating a password policy that emphasizes password length, a primary factor in characterizing password strength recommended by NIST guidelines.
4. Ensure PIV card technology compatibility with on-going and future system development for USPTO next-generation applications, and switch PIV enforcement to a per-user basis, when technically feasible.
5. Finalize the vulnerability-scanning SOP and ensure it includes requirements to verify scanning tools are updated prior to scans and credentialed scanning is performed on physical and virtual machines.
6. Apply the principle of least functionality by developing an authorized open port baseline for system operation, enforce it, and establish an approval procedure for open port requests that deviate from the baseline.
7. Work with USPTO contracting officers to ensure effective government oversight of contractors performing vulnerability assessment scans.
8. Streamline the patch management change-review policies and procedures to allow for timely vulnerability remediation.

Summary of Agency Response and OIG Comments

In response to our draft report, USPTO concurred with all recommendations, noting that USPTO is currently taking actions to address each recommendation. We have included USPTO's formal response as appendix C of this report.

Appendix A: Objective, Scope, and Methodology

Our audit objective was to determine whether USPTO has adequately managed its Active Directory to protect mission critical systems and data.

The scope of this audit included the following USPTO information systems:

1. ESS, which provides the following services to USPTO: Active Directory, Role-Based Access Control System, email, endpoint protection, fax, and SharePoint.
2. Enterprise Windows Services, which is an infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions.

We reviewed Active Directory objects related to account access controls and internal security controls significant within the context of our audit objective. Due to the complexity of USPTO's more than 260,000 Active Directory objects that were accumulated over the years, our technical analysis focused on selected Active Directory groups that have significant privileges. In addition, we employed a comprehensive methodology to validate USPTO security practices for securing 12 domain controllers, as well as hypervisors that host these domain controllers. Specifically, we judgmentally selected and reviewed the implementation status of fundamental security controls defined in NIST Special Publication 800-53, Revision 4, including access control, configuration management, vulnerability scanning, and flaw remediation.

To do so, we:

- reviewed system-related artifacts, including policy and procedures, planning documents, and other materials;
- interviewed USPTO officials, including system owners, IT security and operations staff, and management;
- deployed software tools to analyze the password strength and the selected Active Directory objects, and identified those with privileged access;
- analyzed vulnerability scanning results conducted by USPTO from the second quarter of FY 2017 through the second quarter of FY 2018;

We reviewed USPTO's compliance with the following applicable internal controls, provisions of law, regulation, and mandatory guidance:

- The Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551, et seq.
- U.S. Department of Commerce IT Security Program Policy[24]
- Applicable Commerce Information Technology Requirements (CITR):

[24] DOC, *Information Technology Security Program Policy*. Washington, DC: DOC, 2014, 3:2.

  - CITR-016, Vulnerability Scanning and Patch Management
  - CITR-021, Password Management
- NIST Special Publications:
  - 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
  - 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*

We also used industry best practices as criteria for the review and testing of proper Active Directory configuration.

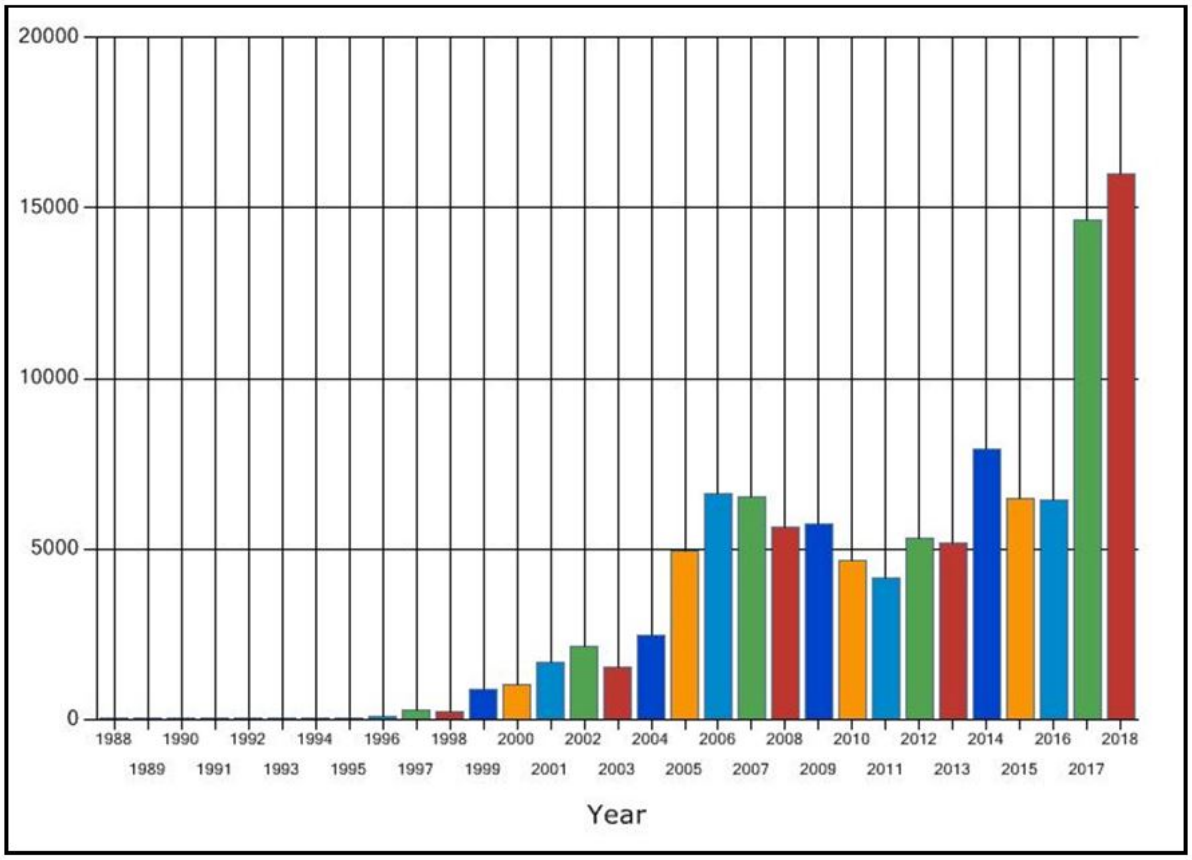
We collected computer-generated data, including Active Directory data and vulnerability scanning results, generated by widely used vendor software tools. Our work involved technical analysis, interviewing knowledgeable USPTO officials, and providing them with the analytical results to eliminate the possibility of false positive results. We determined that the data were sufficiently reliable for the purposes of this report.

We conducted our fieldwork from February to November 2018 at USPTO headquarters in Alexandria, Virginia. We performed this audit under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. App.), and Department Organization Order 10-13, dated April 26, 2013, and 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.

Appendix B: National Vulnerability Database Statistics

NIST manages a comprehensive list of all known vulnerabilities called the National Vulnerability Database (NVD).[25] As of December 2018, this database had more than 110,000 entries, with more than 16,000 from 2018 alone.[26] Figures B-1 and B-2 below show the number of vulnerabilities that have been discovered by year, and by month for 2018, respectively. They illustrate an upward trend as vulnerabilities become more prevalent over time. This database is updated daily as new vulnerabilities are discovered.

Figure B-1. NVD Vulnerabilities by Year



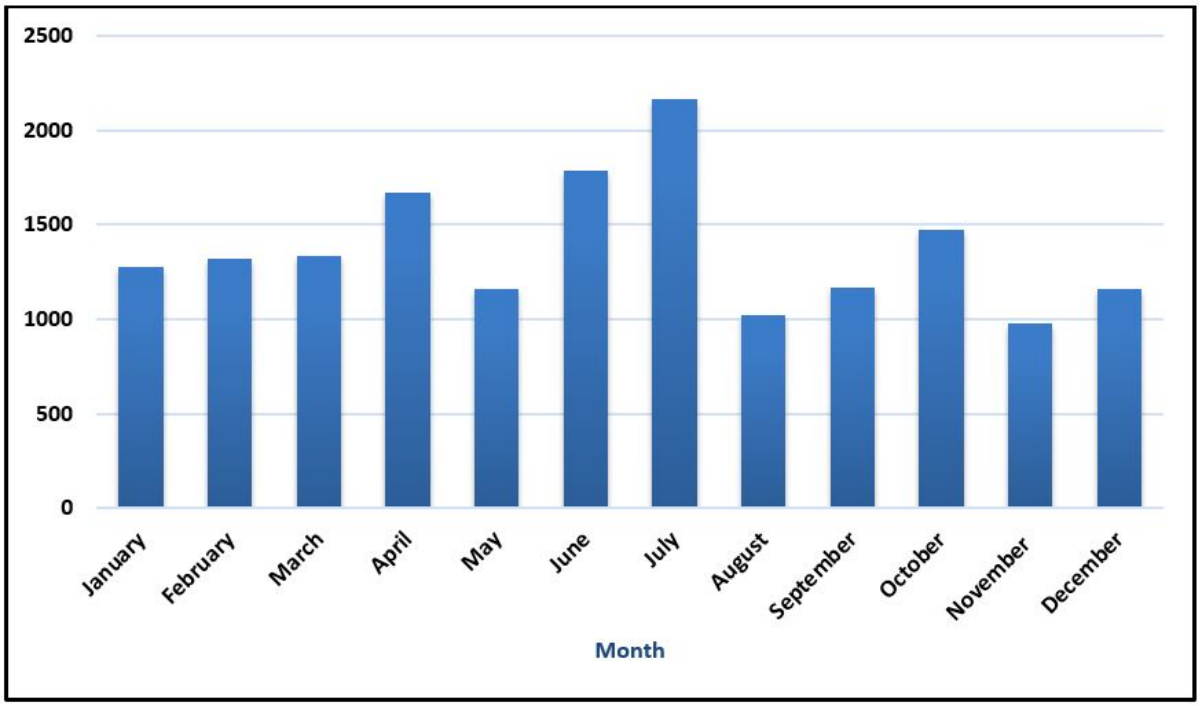
Source: NVD[27]

[25] The NVD can be accessed here: https://nvd.nist.gov/general.

[26] NIST. *National Vulnerability Database* [online]. https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all (accessed December 18, 2018).

[27] Ibid.

Figure B-2. NVD Vulnerabilities by Month 2018



Source: OIG analysis [28]

[28] Derived from National Vulnerability Database statistics.

Appendix C: Agency Response

UNITED STATES PATENT AND TRADEMARK OFFICE

DEPUTY UNDER SECRETARY OF COMMERCE FOR INTELLECTUAL PROPERTY AND
DEPUTY DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE

MAY 15 2019

MEMORANDUM FOR Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

FROM: Laura A. Peter
Deputy Under Secretary of Commerce for Intellectual Property
and Deputy Director of the U.S. Patent and Trademark Office

SUBJECT: Response to Draft Report, *Inadequate Management of Active Directory Puts USPTO's Mission at Significant Cyber Risk* (April 2019)

Executive Summary

Thank you for reviewing the United States Patent and Trademark Office (USPTO) information technology (IT) systems. We greatly appreciate your efforts, and that of your staff, in examining specifically the USPTO Windows Active Directory system.

After careful consideration, we concur with the recommendations made in the report. The detailed responses to each recommendation are below, and the following provides a brief overview of the USPTO's use of IT systems to support its mission.

The USPTO is a fee-funded and metrics-driven organization dedicated to fostering innovation, competitiveness, and economic growth. It supports United States innovators and entrepreneurs by providing high quality and timely examinations of patent and trademark applications, and depends on an IT infrastructure to support its mission. Given the production-based nature of the USPTO business process, patent and trademark examiners are entirely dependent on reliable access to USPTO IT systems to provide services to stakeholders. Any IT system interruption, or downtime, risks productivity and the USPTO's ability to fulfill its mission. In order to ensure that its IT systems are secure and reliable, the USPTO strives to follow Federal Information Security Management Act (FISMA) 2014 (Public Law 113-283) guidance, conducting annual assessments and performing security activities in accordance with the agency's continuous monitoring process. The USPTO continues to re-write and redesign business applications and support infrastructure in order to transform legacy IT systems that have unsupported components to next generation systems. The unsupported elements of legacy systems affect components throughout the enterprise. These efforts are expected to continue through Fiscal Year 2022.

The USPTO is continually considering new means to improve its IT infrastructure in order to fulfill its mission to stakeholders while following applicable cybersecurity policies and best practices.

In response to the issues specifically raised in the report, the USPTO has updated the scanning Standard Operating Procedure (SOP) to ensure updated scanning tools are being used to perform credentialed scans, password policy requirements are being enforced, and unauthorized ports have been disabled. The USPTO has also reviewed its security controls and taken steps to improve its processes and procedures to reduce risk and conform to best practices.

In summary, the USPTO appreciates and concurs with the recommendations in your report, which we will use to further the improvement efforts currently underway. Our response to each recommendation is discussed in detail below, and USPTO provided technical comments under a separate cover.

Response to Recommendations

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of USPTO (1): *Immediately (1) reevaluate the current Active Directory configuration based on users' roles and responsibilities, (2) reorganize Active Directory user groups based on job functions, and (3) remove any unneeded privileges.*

USPTO Response:
USPTO concurs with this recommendation. USPTO has been actively assessing account information in Active Directory (AD) for role and privilege needed. With the IG's assistance, a significant "container" for admin accounts was reviewed and was reduced by over fifty-five percent. Work continues to reduce the membership. Non-human accounts are under review and have already been significantly reduced as well. However, the work continues with increasing attention to role-based assignments. A new process was introduced in January 2019 to review and vet the continued need of domain admin human and non-human accounts.

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of USPTO (2): *Eliminate weak credential encryption to the maximum extent possible. For those applications that currently do not support strong encryption, implement additional compensating controls to protect credentials.*

USPTO Response:
USPTO concurs with this recommendation. The accounts of concern belong to USPTO legacy applications. There are ongoing projects for upgrading legacy applications that are incapable of supporting current strong encryption mechanisms. USPTO has come up with a Watch List to track and monitor as to which legacy applications are using these accounts. Additional mitigating measures include vetting of domain admin and non-human accounts for continued need and eliminating the stale ones.

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of USPTO (3): *Ensure that all passwords meet the standards set by Department and USPTO policies or implement additional compensating controls to protect them. Furthermore, consider incorporating a password policy that emphasizes password length, a primary factor in*

characterizing password strength recommended by NIST guidelines.

USPTO Response:
USPTO concurs with this recommendation. Operations is reaching out to the application owners which have used passwords for their applications based on the requirements in place at the time when the legacy products were developed to request that they be extended to be compliant with current password policy. In addition, USPTO is actively reviewing NIST 800-63B and how this new guidance would significantly update the current password policy. Additional mitigating measures include vetting of domain admin and non-human accounts for continued need and eliminating the stale ones.

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of USPTO (4): *Ensure PIV card technology compatibility with on-going and future system development for USPTO next-generation applications, and switch PIV enforcement to a per-user basis, when technically feasible.*

USPTO Response:
USPTO concurs with this recommendation. USPTO is not yet able to deploy multi-factor authentication on the per-user level due to several of our major applications not being able to utilize single sign-on. This includes our ticketing system (ITSM/Remedy), Email, Skype for Business, and other legacy systems. Even though these systems do utilize the USPTO Active Directory for authentication, they are not set to utilize single sign-on. USPTO will develop a roadmap for migrating or transitioning legacy applications to single sign-on.

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of USPTO (5): *Finalize the vulnerability-scanning SOP and ensure it includes requirements to verify scanning tools are updated prior to scans and credentialed scanning is performed on physical and virtual machines.*

USPTO Response:
USPTO concurs with this recommendation. In order to ensure our scanning tools are up to date before scans are performed, the Tenable Security Center instance at USPTO was configured to automatically download and update scanning plugins as updated by Tenable. In addition, the USPTO Cybersecurity Scan Process SOP has been updated to include language specifically addressing the need to verify that scan tools and policies are updated prior to scanning. Language is also added in the SOP that denotes the importance of verifying credentialed scans are successful on both physical and virtual machines and hypervisors and of troubleshooting credential issues when identified as part of the scanning process.

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of USPTO (6): *Apply the principle of least functionality by developing an authorized open port baseline for system operation, enforce it, and establish an approval procedure for open port requests that deviate from the baseline.*

USPTO Response:

USPTO concurs with this recommendation. USPTO has been focused on the ports and protocols question for several months. A detailed list has been compiled of ports required for assorted functions from operating systems and middleware. The scan content has been adjusted to include the associated processes for ports that are "listening," which are different than ports that are merely not closed. USPTO is using the new baseline of ports with some recent cases of port identification POAMs to evaluate its usefulness and tweak as needed. The baseline includes information on static and dynamic ports, which has a significant impact on required open port ranges. Ports and protocols are defined for the UNIX platforms but were missing from pre-2016 Windows server baselines. USPTO is addressing this oversight.

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of USPTO (7): *Work with USPTO contracting officers to ensure effective government oversight of contractors performing vulnerability assessment scans.*

USPTO Response:
USPTO concurs with this recommendation. USPTO's Cybersecurity Division is currently undergoing a re-compete of the contract that includes contractor support for vulnerability assessment scans services. As part of the re-compete effort, the Cybersecurity Division has been engaged with the Office of Procurement and Vendor Management Division to move the new contract to a performance-based contract. As part of the Statement of Work (SOW) for the new contract, USPTO has defined performance requirements as part of the SOW's Surveillance Plan. The Cybersecurity Division has also backfilled a vacant Full-time Equivalent (FTE) position that performs as a subject matter expert, is the main Government Point of Contact (POC) for the USPTO Cybersecurity Division's Vulnerability Scanning Program, and provides oversight to the contractor vulnerability scanning team.

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of USPTO (8): *Streamline the patch management change-review policies and procedures to allow for timely vulnerability remediation.*

USPTO Response:
USPTO concurs with this recommendation. The USPTO Enterprise Directory Services (EDS) group is actively working to apply patches and remediate vulnerabilities in a timely manner.

Conclusion

In closing, we appreciate your work and thank the Assistant Inspector General for Audit and Evaluation for providing us with this report. USPTO is always looking to improve its processes and drive the best outcomes on behalf of its stakeholders. This information will help us achieve those goals. USPTO and the Office of the Chief Information Officer have made improvements to implement the report's recommendations and are confident in our abilities to satisfy these recommendations in a timely manner. We look forward to working with your office in the future as we continue our efforts to improve our IT security and operations practices.

If additional information is needed please contact:

Don Watson by phone at (571) 272-8130 or by e-mail at Don.Watson@USPTO.GOV
OCIO Senior Information Security Officer (SISO) & Cybersecurity Division Director

Saji Ranasinghe by phone at (571) 272-5249 or by email at Saji.Ranasinghe@USPTO.GOV
OCIO Cybersecurity Authorizations and Compliance Branch Chief