U.S. PATENT AND TRADEMARK OFFICE

Inadequate Security Practices, Including Impaired Security of Cloud Services, Undermine USPTO's IT Security Posture

FINAL REPORT NO. OIG-17-021-A
MARCH 24, 2017

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

FOR PUBLIC RELEASE

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

March 24, 2017

MEMORANDUM FOR: John Owens II
Chief Information Officer, USPTO

Allen Crawley

FROM: Allen Crawley
Assistant Inspector General for Systems Acquisition
and IT Security

SUBJECT: *Inadequate Security Practices, Including Impaired Security of Cloud Services, Undermine USPTO's IT Security Posture*
Final Report No. OIG-17-021-A

Attached is our final report on OIG's audit of USPTO's information technology (IT) security posture. Our objective was to determine whether key security measures are in place to adequately protect USPTO systems that utilize databases to store business information.

We found that USPTO's IT security posture was undermined due to inadequate security practices, including impaired security of cloud services. Specifically, USPTO (1) failed to implement the required security controls for cloud-based subsystems; (2) used non-Federal Risk and Authorization Management Program (FedRAMP) compliant cloud services without proper security assurance; and (3) deficiently implemented fundamental security controls, which increased the cybersecurity risk of USPTO systems.

We have summarized the agency's response to our draft report, as well as included it as appendix C. 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).

In accordance with Departmental Order 213-5, please submit to us—within 60 calendar days of the date of this memorandum—an action plan that responds to the recommendations of this report.

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) 482-1855 or Dr. Ping Sun, Director for IT Security, at (202) 482-6121.

Attachment

cc: Rod Turk, Acting Chief Information Officer
Welton Lloyd, Audit Liaison, USPTO
Maria Stanton-Dumas, Audit Liaison, Office of the Chief Information Officer

Report in Brief

March 24, 2017

U.S. PATENT AND TRADEMARK OFFICE

Inadequate Security Practices, Including Impaired Security of Cloud Services, Undermine USPTO's IT Security Posture

OIG-17-021-A

WHAT WE FOUND

We found that USPTO's IT security posture was undermined due to inadequate security practices, including impaired security of cloud services. Specifically, USPTO (1) failed to implement the required security controls for cloud-based subsystems; (2) used non-Federal Risk and Authorization Management Program (FedRAMP) compliant cloud services without proper security assurance; and (3) deficiently implemented fundamental security controls, which increased the cybersecurity risk of USPTO systems.

WHAT WE RECOMMEND

We recommend that the USPTO Chief Information Officer do the following:

1. Take immediate action to implement and assess required security controls for the Global Patent Search Network, or discontinue operation of the subsystem.
2. Follow the National Institute of Standards and Technology Risk Management Framework process to ensure that required security controls are properly implemented and assessed on all cloud-based systems when using FedRAMP-compliant services.
3. Establish processes to develop and maintain an accurate inventory of all cloud-based servers, and conduct routine vulnerability scanning, as required by Department and USPTO policies.
4. Ensure that all applicable security controls are implemented and assessed for all non-FedRAMP compliant services already in-use, or discontinue use of such services.
5. Establish processes to determine the feasibility of obtaining sufficient assurance that the required controls are adequately implemented and assessed prior to using cloud-based services.
6. Evaluate current strategy of replacing unsupported server operating systems, and develop and implement a plan to prioritize available resources for the component upgrade or replacement.
7. Ensure that unsupported databases are upgraded or replaced in a timely manner.
8. Ensure that accurate inventories of hardware and software products are established and maintained.
9. Establish a process to ensure effective coordination between the Cybersecurity Division and operation teams to timely share critical security information, such as credentials and vulnerability scanning reports.
10. Establish vulnerability scanning procedures that require credentialed scanning of all system components as required by Department and USPTO policies.
11. Ensure that passwords for user and database administrator database accounts meet the standards set by Department and USPTO policies.
12. Ensure that unauthorized ports are disabled for all USPTO systems.

Background

The United States Patent and Trademark Office (USPTO) is the nation's single entity that examines, grants, and registers patents and trademarks to individual inventors, organizations, and businesses. Its mission is fostering innovation, competitiveness, and economic growth domestically and abroad by delivering high quality and timely examination of patent and trademark applications, guiding domestic and international intellectual property policy, and delivering intellectual property information and education worldwide. To support this mission, USPTO relies on its 56 information systems, some of which use cloud computing services.

Cloud computing is a way for acquiring and delivering computing services. It enables on-demand access to shared computing resources with the goal of reducing information technology (IT) costs. To help achieve these efficiencies, the Office of Management and Budget issued a "Cloud First" policy that required each agency's chief information officer to implement a cloud service whenever there was a secure, reliable, cost-effective option.

Why We Did This Review

We conducted this audit to determine whether key security measures are in place to adequately protect USPTO systems that utilize databases to store business information.

Contents

COVER: Detail of fisheries pediment,
U.S. Department of Commerce headquarters,
by sculptor James Earle Fraser, 1934

Introduction

The United States Patent and Trademark Office (USPTO) is the nation's single entity that examines, grants, and registers patents and trademarks to individual inventors, organizations, and businesses. Its mission is fostering innovation, competitiveness, and economic growth domestically and abroad by delivering high quality and timely examination of patent and trademark applications, guiding domestic and international intellectual property policy, and delivering intellectual property information and education worldwide. To support this mission, USPTO relies on its 56 information systems, some of which use cloud computing services.

Cloud computing is a way for acquiring and delivering computing services. It enables on-demand access to shared computing resources with the goal of reducing information technology (IT) costs. To help achieve these efficiencies, the Office of Management and Budget (OMB) issued a "Cloud First" policy[1] that required each agency's chief information officer (CIO) to implement a cloud service whenever there was a secure, reliable, cost-effective option.

To help achieve adequate security for cloud services, the government-wide Federal Risk and Authorization Management Program (FedRAMP) was established to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud services. Specifically, FedRAMP provides approved authorization packages,[2] which could be leveraged by the authorizing officials to make risk-based decisions regarding the use of cloud services. This "do once, use many times" approach saves cost and time required to conduct redundant agency security assessments. The FedRAMP policy memorandum[3]—issued by OMB in December 2011—mandates FedRAMP compliance for all cloud services used by the federal government.

The Federal Information Security Modernization Act of 2014, Pub. L. No. 113–283, an update of the Federal Information Security Management Act of 2002, Pub. L. No. 107–347, requires the Department and its bureaus to secure their IT systems through the use of cost-effective management, operational, and technical controls. This responsibility applies to all IT systems, including those using cloud computing services.

The National Institute of Standards and Technology (NIST) outlined a six-step process to manage risks throughout an information system's life cycle, known as the Risk Management Framework (RMF).[4] Federal agencies have been required to follow the process since February 2010. This framework includes security control implementation and assessment and system authorization based upon a risk-based decision.

[1] See OMB, February 8, 2011. *Federal Cloud Computing Strategy*. Washington, DC: OMB.
See also CIO Council and Chief Acquisition Officers Council, February 24, 2012. *Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service*. Washington, DC: CIO Council.

[2] Authorization packages include, at minimum, the Security Plan, Security Assessment Report, Plan of Action and Milestones, and a Continuous Monitoring Plan. See OMB, December 8, 2011. *Security Authorization of Information Systems in Cloud Computing Environments*. Washington, DC: OMB.

[3] OMB, December 8, 2011. *Security Authorization of Information Systems in Cloud Computing Environments*. Washington, DC: OMB.

[4] NIST, February 2010. *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST SP 800-37, Rev 1. Gaithersburg, MD: NIST.

Objective, Findings, and Recommendations

We conducted this audit to determine whether key security measures are in place to adequately protect USPTO systems that utilize databases to store business information. We judgmentally selected 7 of 56 USPTO systems that support the mission of granting U.S. patents and registering trademarks. (See appendix B.) Two of these selected systems utilize commercial cloud computing services. Our review focused on fundamental security practices and control implementations on these selected systems. See appendix A for further details regarding our objective, scope, and methodology.

We found that USPTO's IT security posture was undermined due to inadequate security practices, including impaired security of cloud services. Specifically, USPTO (1) failed to implement the required security controls for cloud-based subsystems; (2) used non-FedRAMP compliant cloud services without proper security assurance; and (3) deficiently implemented fundamental security controls, which increased the cybersecurity risk of USPTO systems.

I. USPTO Failed to Implement the Required Security Controls for Cloud-Based Subsystems

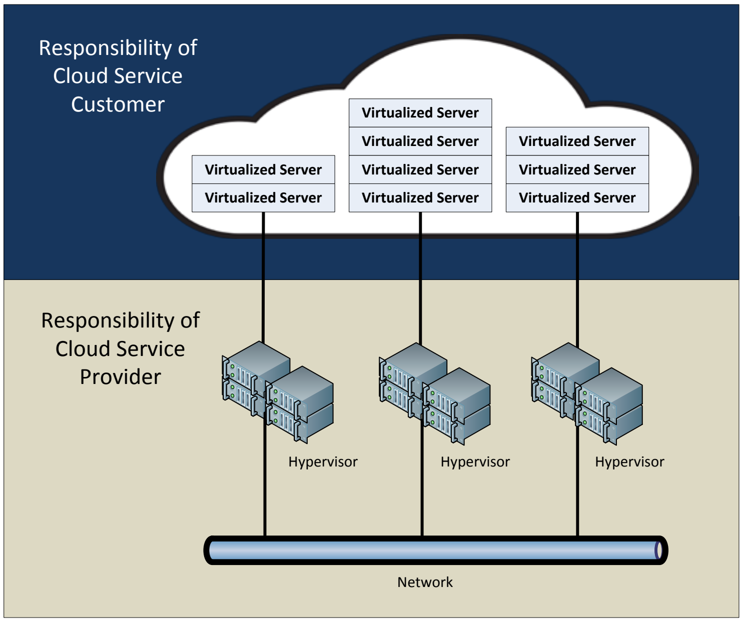
In 2013, USPTO began using a cloud-based service to host the Global Patent Search Network (GPSN)—a subsystem of the Patent End-to-End (PE2E) system that provides public access to translations of the Chinese patent data distributed by the State Intellectual Property Office of China and does not contain USPTO patent application data. USPTO decided to deploy GPSN on a FedRAMP-compliant infrastructure as a service (IaaS)[5] provided by a commercial cloud vendor. To achieve FedRAMP compliance, the IaaS was assessed by a third-party assessment organization (3PAO) and granted an authorization to operate (ATO) by the Department of Health and Human Services (HHS).[6] USPTO leveraged this ATO for its own use of the cloud service. However, because this service is an IaaS, the commercial vendor is only responsible for providing secure infrastructure, such as hypervisors,[7] networking, and physical storage facilities. As a customer, USPTO used this infrastructure to deploy virtualized servers, such as web servers and application servers. Therefore, USPTO was responsible for implementing required security controls for these virtualized servers (see figure 1).

[5] IaaS is a capability provided to a consumer to provision processing, storage, and other computing resources where the consumer is able to deploy software, such as operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but does have control over the deployed software.

[6] A 3PAO is an accredited organization that performs initial and periodic assessments of cloud providers to ensure they meet FedRAMP requirements. HHS is the first federal agency to grant this cloud service an ATO.

[7] The hypervisor is a program that allows multiple operating systems to share a single hardware server. Each operating system appears to exclusively use the hardware server's processor, memory, and other resources.

Figure 1. Cloud IaaS Customer and Service Provider Responsibilities



Source: OIG developed. This figure is a conceptual representation of the generalized responsibility areas for a customer using a cloud IaaS.

We found that required security controls had not been implemented on GPSN because of USPTO's misunderstanding of the scope of its security responsibilities. From system deployment in June 2013 until September 2015, USPTO was unaware of this deficiency of security control implementation because it did not perform security control assessments for GPSN. It was not until the fiscal year (FY) 2016 assessment that USPTO realized required security controls had not been implemented. USPTO then developed corrective actions to address the deficiency. However, those corrective actions were inadequate to address the absence of required security controls. Further, the required vulnerability scanning of virtualized servers deployed on the cloud was never performed due to the lack of an accurate subsystem inventory.

A. *Required security controls were not implemented on GPSN*

Prior to system deployment, USPTO must ensure that all applicable security controls were implemented, as required by NIST 800-53, Rev. 4.[8] In June 2013, USPTO deployed GPSN. To validate that the required security controls were adequately implemented on GPSN, we selected 23 for review.[9] Since GPSN is a low-impact subsystem of the moderate-impact PE2E system, only 16 of the 23 controls were applicable. We found that none of the 16 applicable controls had been implemented. Further, we found 15 of

[8] Federal Information Processing Standards Publication 200: *Minimum Security Requirements for Federal Information and Information Systems* requires federal agencies to meet the minimum security requirements through the use of the security controls in accordance with NIST Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

[9] We selected 23 critical controls that apply to USPTO moderate-impact systems. See appendix A for our detailed methodology.

them incorrectly relied upon the cloud service provider for implementation for over 3 years.

USPTO's misplaced reliance on the cloud service provider to implement controls was because of its misunderstanding of customer responsibilities. However, USPTO's responsibility was explicitly stated in the cloud provider's security document—the Customer Responsibility Matrix (CRM)[10]—which was available to USPTO in December 2013. Further, USPTO's misunderstanding of their customer responsibilities was worsened by not conducting security control assessments for GPSN from system deployment in 2013 through September 2015. Consequently, none of the selected GPSN critical security controls were implemented.

B. Planned corrective actions did not address actual implementation of the required security controls

In September 2015, USPTO conducted the FY 2016 annual security assessment[11] of the PE2E system, which included GPSN. This assessment found that USPTO had incorrectly relied upon the service provider to implement required security controls for GPSN. To address this newly discovered deficiency, USPTO developed a corrective action plan. However, this plan only addressed updating the system security documentation but did not address the actual implementation or assessment of the required controls, all part of proper implementation of the RMF process.

We asked USPTO officials how this plan would ensure that the required security controls were actually implemented. They acknowledged that their planned actions only addressed updating system security documentation. They also indicated that the control implementations would not be assessed until the next annual security assessment later in 2016. However, in September 2016, USPTO again insufficiently assessed GPSN which resulted in assessors stating that 10 of the 12 controls evaluated had insufficient evidence to complete the assessment. Consequently, required security controls for GPSN will remain unimplemented until a sufficient assessment identifies the problem and adequate corrective actions are performed.

C. Vulnerability scanning did not occur for cloud-based subsystems

Department and USPTO policies require quarterly vulnerability scanning of system components.[12] We found that GPSN servers being hosted by the cloud provider were never scanned since system deployment in 2013. This was due to USPTO's lack of maintaining an accurate inventory of the servers deployed in a cloud environment. We also found a similar issue on another PE2E subsystem being hosted on FedRAMP-

[10] The CRM is a document that is provided by the cloud service provider which defines the responsibilities of security control implementation for both the cloud service provider and the customer.

[11] USPTO completed PE2E's 2016 fiscal year annual assessment during September 2015.

[12] Examples of system components include servers and workstations.

compliant IaaS, the Cooperative Patent Classification-Intellectual Property (CPC-IP).[13] For both systems, USPTO did not perform vulnerability scanning or maintain an accurate inventory of the cloud-deployed servers.

Establishing and maintaining an inventory of servers being hosted on a commercial cloud presents challenges, which is a result of the dynamic nature of a cloud computing environment. However, without the maintenance of an accurate system inventory—as required by Department and USPTO policy—vulnerability scanning cannot be properly completed. By not scanning for vulnerabilities, the potential security weaknesses were left unknown and greatly diminished the security posture of the cloud-based system.

II. USPTO Used Non-FedRAMP Compliant Cloud Services without Proper Security Assurance

In December 2011, OMB mandated FedRAMP compliance for all cloud services used by the federal government by June 2012.[14] However, beginning in September 2012, during development of its next generation systems—PE2E and Trademark Next Generation (TMNG)—USPTO decided to use non-FedRAMP compliant software as a service (SaaS),[15] such as application monitoring, e-mail, notification, and database services. These services have not been independently evaluated by a FedRAMP 3PAO, and have not received an ATO that could be leveraged by USPTO. Therefore, USPTO is solely responsible for ensuring that all required security controls are implemented and assessed, as required, for FedRAMP compliance.

We found that USPTO accepted the risk to use an unsecure non-FedRAMP compliant cloud service despite known, significant security deficiencies. Also, USPTO did not have a viable path forward to achieve compliance of other non-FedRAMP approved cloud services.

A. USPTO improperly accepted the risk to use an unsecure non-FedRAMP compliant cloud service

In August 2015, USPTO granted an Interim Authorization to Test (IATT)[16] for a cloud-based database service, as part of the CPC-IP subsystem. During testing of the cloud

[13] CPC-IP is a low-impact subsystem of the PE2E system that provides a shared repository for all patents schemes approved by USPTO and the European Patent Office. At the time of CPC-IP deployment into a production environment in May 2016, it was authorized as the standalone system named "Cooperative Patent Classification - Intellectual Property Office Collaboration Tools."

[14] "For all currently implemented cloud services or those services currently in the acquisition process prior to FedRAMP being declared operational, security authorizations must meet the FedRAMP security authorization requirement within 2 years of FedRAMP being declared operational." See OMB, December 8, 2011. *FedRAMP Policy Memorandum*. Washington, DC: OMB.

[15] SaaS is a capability provided to a consumer to use the provider's applications running on a cloud infrastructure. The applications are often accessible via a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the exception of limited user-specific application configuration settings.

[16] IATT is a special type of authorization decision allowing an information system to operate in an operational environment in order to test the system with actual operational (i.e., live) data for a specified period. The authorizing official grants an IATT only when the operational environment or live data are required to complete

service, significant security deficiencies were found by the 3PAO. Specifically, after testing only 43 of 325 controls,[17] the 3PAO found 43 moderate and 68 low security deficiencies. Subsequently, the cloud service was explicitly rejected by HHS from inclusion in the list of FedRAMP-approved services. As a result, USPTO's Cybersecurity Division recommended moving to a USPTO-approved configuration baseline and discontinuing use of the cloud service. However, the system owner of CPC-IP concluded that using the cloud service or USPTO's own database would have similar levels of risk. In May 2016, despite its significant security deficiencies, the authorizing official accepted the risks of the cloud service and continued its use in the fully authorized production environment of CPC-IP.

B. USPTO did not have a viable path forward to achieve compliance for non-FedRAMP approved cloud services

In addition to the cloud-based database service, USPTO has also used other non-FedRAMP compliant cloud services as part of its cloud-based systems, such as application monitoring, e-mail, notification, and management services. According to the OMB December 2011 FedRAMP policy memorandum and Department policy, these SaaS are required to be FedRAMP-compliant when used by USPTO.[18] As previously mentioned in this report, when a cloud service is not FedRAMP-compliant, USPTO cannot leverage an existing ATO. Instead, USPTO is responsible for ensuring all FedRAMP-required controls have been implemented and assessed so that the service may be authorized to operate by USPTO's authorizing official.

To do so, USPTO must gather the necessary information from the provider to ensure that required controls have been correctly implemented and properly assessed. Before a cloud service has achieved FedRAMP compliance, the provider generally does not release IT security-related documentation to its customers because of the proprietary nature of non-FedRAMP compliant SaaS. To assist customers in documenting how security controls for non-FedRAMP compliant SaaS are implemented on their system, the provider made results of various regulatory compliance reviews—such as SOC[19] and ISO 27001[20]—available. However, after evaluating the regulatory compliance reviews, USPTO concluded that the reviews did not contain sufficient information to ensure that the required security controls were correctly implemented or assessed. As a result,

specific test objectives. The IATT allows organizations to assess functional and security requirements within a system's intended environment during development.

[17] FedRAMP requires the implementation and assessment of 325 controls for a moderate impact level.

[18] U.S. Department of Commerce, March 29, 2016. *FedRAMP Applicability*, Commerce Information Technology Requirement 024 (CITR-024). Washington, DC: DOC.

[19] SOC (Service Organization Controls) are reports intended to provide information and assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

[20] International Organization for Standardization (ISO) 27001 is a standard to keep information assets secure by providing requirements for an information security management system.

USPTO was left with no viable path forward to ensure all FedRAMP-required controls had been implemented by the cloud service provider.

Conclusion of Findings I and II

The issues identified in findings I and II illustrate the challenges and confusion USPTO had when using commercial cloud-based services, which resulted in the impaired security implementation for its cloud-based systems. The GPSN subsystem was USPTO's first IT system to use a commercial cloud service. According to USPTO, this was an ideal trial-run because of the low risk nature of the low-impact GPSN subsystem. However, USPTO has knowingly neglected the security requirements for GPSN by (1) not implementing required security controls; (2) taking inadequate remediation actions; and (3) never tracking and scanning cloud-deployed servers. This history of unawareness and neglect of security for the cloud-based system demonstrated the breakdown of a meaningful trial-run of cloud services. As evidenced, the CPC-IP system was deployed nearly 3 years after GPSN, yet we saw similar fundamental deficiencies in the secure implementation of the cloud-based system. Therefore, this trial was a deficient test for future cloud deployments.

During this audit's exit conference with USPTO on October 18, 2016, USPTO acknowledged our concerns on using commercial cloud services and indicated that it will develop a plan to discontinue use of all cloud services affected by this audit. According to the USPTO CIO, the decision to cease using both IaaS and SaaS offered by the provider is based upon the unbounded risk the authorizing official must accept when using non-FedRAMP compliant services. Specifically, while the infrastructure cloud services are FedRAMP-approved and risk is clearly defined, the management services to administer the infrastructure cloud services are not FedRAMP-approved.

Recommendations

We recommend that the USPTO Chief Information Officer do the following:

1. Take immediate action to implement and assess required security controls for GPSN, or discontinue operation of the subsystem.
2. Follow the NIST RMF process to ensure that required security controls are properly implemented and assessed on all cloud-based systems when using FedRAMP-compliant services.
3. Establish processes to develop and maintain an accurate inventory of all cloud-based servers, and conduct routine vulnerability scanning, as required by Department and USPTO policies.
4. Ensure that all applicable security controls are implemented and assessed for all non-FedRAMP compliant services already in-use, or discontinue use of such services.
5. Establish processes to determine the feasibility of obtaining sufficient assurance that the required controls are adequately implemented and assessed prior to using cloud-based services.

III. USPTO Deficiently Implemented Fundamental Security Controls, Which Increased the Cybersecurity Risk of USPTO Systems

USPTO relies on multiple information systems to support its critical mission of granting patents and trademarks. Some of these systems—such as Enterprise UNIX Servers (EUS) and Database Services (DBS)—are IT infrastructure systems that provide servers and databases to host application systems and store mission-critical information. Application systems support various steps in the process of granting patents and trademarks. In addition, USPTO relies heavily on virtualization technology to host servers and databases. For example, in FY 2015, the EUS system contained over 110 hypervisors, which are critical components that support virtualization of IT infrastructure.

USPTO systems are maintained by various operation teams—such as the individual application teams, the Database Services Branch, and the Server and Storage Services Branch—while the vulnerability scanning and security documentation maintenance are handled by the Cybersecurity Division. The operation teams provide information to the Cybersecurity Division to create and update the security documentation that serves as a base for security control assessment. The Cybersecurity Division provides vulnerability scan reports to the operation teams. For this reason, effective coordination among these teams is essential to ensure that adequate security is properly implemented.

We reviewed fundamental security controls on seven selected systems, which included five application systems: USPTO's next-generation modernization systems (PE2E and TMNG); the legacy systems (Patent Search System-Primary Search and Retrieval (PSS-PS), Patent Search System-Specialized Search and Retrieval (PSS-SS), and Trademark Processing System-External Systems (TPS-ES)); and infrastructure systems (EUS and DBS). See appendix B for system descriptions.

We identified unsupported server operating systems and databases within USPTO's IT infrastructure. We also found that the vulnerability scanning performed by USPTO was not comprehensive and missed a majority of hypervisors and databases. Furthermore, credential scanning was not consistently employed.

In addition, we found weak passwords for both database user and database administrator (DBA) accounts. We also identified unauthorized open ports and running services on application system components.

A. Unsupported server operating systems and databases resulted in persistent vulnerabilities within USPTO's IT infrastructure

Patching software products, such as server operating systems and databases, to remediate security vulnerabilities is required by Department and USPTO policies, and is considered one of the best security practices to reduce the risk of compromise. In general, software vendors provide customers with support and patches for their products until a certain date. Customers must upgrade to the next version of the product to continue to receive patches.

We reviewed the versions of software products installed on the EUS and DBS systems. We found that 70 EUS servers supporting USPTO legacy systems had operating systems that were no longer supported. Therefore, potential critical vulnerabilities for these servers will remain until the operating systems are upgraded. In addition, 21 databases operating within the DBS system were unsupported, and 16 of them were susceptible to critical vulnerabilities, including Structured Query Language (SQL) injection.[21] Seven of these databases have been unsupported since July 2010.

For EUS, USPTO was fully aware of these unsupported system components, and had planned to replace them since 2012. However, USPTO repeatedly extended the replacement deadline by simply accepting the risk. The main reason for the delay—according to the USPTO CIO—was due to business needs requiring the legacy systems continued operation and the competing resources USPTO has to commit to the migration effort. For DBS, inadequate coordination between the operation teams responsible for maintaining databases and maintaining the applications running within these databases led to a delay in upgrading database version.

B. Scanning practices were inadequate to identify vulnerabilities

According to USPTO policy, all system components are to be scanned quarterly. However, USPTO implemented an inadequate scanning process that only scanned a subset of EUS system components each quarter, with a goal of scanning all components over the course of a year. To assess USPTO's scanning practices, we reviewed all EUS scanning reports conducted in FY 2015. We found that 85 percent (105 out of 123) of the hypervisors within EUS had not been scanned in the entire year. Hypervisors are critical system components that host virtualization infrastructure to support USPTO application systems. By not scanning hypervisors, potential security weaknesses were unknown and unremediated, thus increasing the security risk that jeopardized USPTO's mission.

By using a database scanning tool, USPTO planned to scan all databases within DBS each quarter. We reviewed the scanning reports conducted in the fourth quarter of FY 2016, and focused on one type of database[22] that is widely deployed at USPTO. We found 66 percent (116 out of 176) of the databases had not been scanned. Similar to hypervisors, when databases are not scanned, the potential for unknown and unremediated security weaknesses negatively affects confidentiality, integrity, and availability of data stored on these databases.

Not scanning such a large number of system components and databases was due to the lack of effective coordination between the EUS operation team and the Cybersecurity Division, as well as the DBS operation team and the Cybersecurity Division, resulting in incomplete inventory of EUS hypervisors and DBS databases. As required by Department policy, each system should develop and maintain up-to-date inventory of

[21] SQL injection is a vulnerability which allows an attacker to execute a command via a web form to extract, modify, or destroy the data stored in the back-end database.

[22] USPTO uses multiple databases from different vendors.

system components. Since the incomplete inventories were used by the Cybersecurity Division to perform scans of system components and databases, the scans inevitably would miss those not included in the inventories.

Further, when performing a vulnerability scan, it is imperative to use credentials—as required by Department policy[23]—to ensure an accurate and comprehensive vulnerability scan. We found that USPTO did not consistently use credentials to scan 11 percent (79 out of 749) of EUS components in FY 2015. Specifically, these components were scanned with credentials in one quarter, but not during another. According to USPTO, this inconsistency was because the credentials were changed on the system components by the EUS operation team, but the new credentials were not given to the Cybersecurity Division to perform the scan. As a result, components were scanned with invalid credentials, and thus the scanning result did not provide an accurate picture of known vulnerabilities.

C. Weak passwords made databases vulnerable to unauthorized access

Our review of the database scanning reports also identified 13 databases having database user accounts with weak, easily-guessed passwords, including DBA accounts. We tested those accounts by successfully logging into the databases, and confirmed that 19 user accounts and 2 DBA accounts had weak passwords.

We judgmentally selected six accounts to further examine the reasons for having weak passwords. We found three operation teams were responsible for maintaining the applications that utilized these accounts. The teams were either unaware of the deficiency or decided to leave the password unchanged because of the obstacle to change it. Specifically:

- One team was not aware of the two weak DBA account passwords that were originally created to facilitate software installation and vendor customer support. After our inquiry, the DBA accounts were disabled.
- One team was fully aware of one user account, but allowed its continued use. According to the team, there are several hundred reporting products utilizing this password, and it is difficult to manually change the password on each product without disrupting business operations. No action had been taken to change the password.
- One team was not aware of the weak passwords of three user accounts, which had not been changed since October 2012. This deficiency was never discovered because, according to the team, database vulnerability scanning reports were not provided to them by the Cybersecurity Division. After we notified the team, it took action to change the passwords and disable these accounts.

Strong passwords are required by Department and USPTO policies and are necessary to ensure the security of the mission critical data stored on the USPTO databases.

[23] Per CITR-016, *Vulnerability Scanning and Patch Management*, all network addressable devices must be scanned with credentials.

USPTO's use of weak, easily-guessed passwords—especially on DBA accounts—leaves databases vulnerable to unauthorized access or modification.

D. *Unauthorized open ports and running services increased the risk of system compromise*

Ports are entryways into a system component for running services. A service is an application that communicates with another system component through a designated port. Ports that are utilized by a system should be maintained in the system's security documentation by the Cybersecurity Division. The security documentation is then used to authorize the system and support continuous monitoring. Thus, any ports that are undocumented would be unauthorized.

USPTO is required to adhere to the security control requirements defined by NIST. These requirements include the limiting of information systems to the least functionality necessary[24] by disabling all unneeded ports and services.

We reviewed selected system components from 5 application systems and identified 105 unauthorized ports and services on 4 systems. No unauthorized ports and services were found for the selected PE2E system components. USPTO was unsure of the purpose or what services were running on the open ports.

Table 1. Unauthorized Open Ports and Services per System

System	Number of Unauthorized Ports & Services
TMNG	5
TPS-ES	22
PSS-PS	60
PSS-SS	18
PE2E	0
Total	**105**

Source: OIG analysis of USPTO vulnerability scans.

These open ports illustrated the inadequacy of the practice for documenting authorized ports by USPTO teams. Leaving these ports open and potentially unneeded running services increases the risk of system compromise.

[24] NIST, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Rev. 4. Gaithersburg, MD: NIST, F-71.

As illustrated in this finding, the breakdown of coordination resulted in deficient security control implementations, including inadequate vulnerability scanning, weakened database security, and unauthorized open ports. These deficiencies could be significantly minimized if effective coordination occurs between the Cybersecurity Division and operation teams.

In addition, we are especially concerned about the inadequate security practices on EUS and DBS systems because they are critical IT infrastructure systems that provide underlying support to USPTO business functions. Any security vulnerability existing on these systems could result in a serious consequence to USPTO's mission. USPTO must ensure that adequate security is in place to protect its critical IT infrastructure.

Recommendations

We recommend that the USPTO Chief Information Officer do the following:

6. Evaluate current strategy of replacing unsupported server operating systems, and develop and implement a plan to prioritize available resources for the component upgrade or replacement.
7. Ensure that unsupported databases are upgraded or replaced in a timely manner.
8. Ensure that accurate inventories of hardware and software products are established and maintained.
9. Establish a process to ensure effective coordination between the Cybersecurity Division and operation teams to timely share critical security information, such as credentials and vulnerability scanning reports.
10. Establish vulnerability scanning procedures that require credentialed scanning of all system components as required by Department and USPTO policies.
11. Ensure that passwords for user and DBA database accounts meet the standards set by Department and USPTO policies.
12. Ensure that unauthorized ports are disabled for all USPTO systems.

Summary of Agency Response and OIG Comments

In response to our draft report, USPTO concurred with all recommendations and described both completed and planned actions to address each recommendation. USPTO also included technical comments to our draft report, from which we made changes to the final report where appropriate. 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 key security measures are in place to adequately protect USPTO systems that utilize databases to store business information.

We reviewed internal controls significant within the context of our audit objective and employed a comprehensive methodology to validate the security posture of 7 of 56 selected USPTO moderate-impact systems. Specifically, we judgmentally selected and reviewed implementation status of 23 controls defined in NIST Special Publication 800-53, Rev. 4, which are part of the moderate-impact system baseline. However, when we evaluated the control implementation for the low-impact subsystems of the moderate impact system, we selected 16 of 23 controls that are part of low-impact system baseline (see table A-1).

Table A-1. Office of Inspector General-Selected Security Controls

Control Family	Control No.	Control Name	Baseline
Access Control	AC-2	Account Management	Low and Moderate
	AC-3	Access Enforcement	Low and Moderate
	AC-5	Separation of Duties	Moderate
	AC-6	Least Privilege	Moderate
	AC-12	Session Termination	Moderate
	AC-17	Remote Access	Low and Moderate
Audit and Accountability	AU-2	Audit Events	Low and Moderate
	AU-3	Content of Audit Records	Low and Moderate
	AU-6	Audit Review, Analysis, and Reporting	Low and Moderate
Configuration Management	CM-2	Baseline Configuration	Low and Moderate
	CM-3	Configuration Change Control	Moderate
	CM-6	Configuration Settings	Low and Moderate
	CM-7	Least Functionality	Low and Moderate
	CM-8	Information System Component Inventory	Low and Moderate
Identification and Authentication	IA-2	Identification and Authentication (Organizational Users)	Low and Moderate
Planning	PL-2	System Security Plan	Low and Moderate
Risk Assessment	RA-5	Vulnerability Scanning	Low and Moderate

Control Family	Control No.	Control Name	Baseline
System and Communication Protection	SC-8	Transmission Confidentiality and Integrity	Moderate
	SC-13	Cryptographic Protection	Low and Moderate
	SC-28	Protection of Information at Rest	Moderate
System and Information Integrity	SI-2	Flaw Remediation	Low and Moderate
	SI-3	Malicious Code Protection	Low and Moderate
	SI-10	Information Input Validation	Moderate

Source: NIST Special Publication 800-53, Rev. 4, Appendix F (Security Control Catalog)

To do so, we:

- reviewed system-related artifacts, including policy and procedures, planning documents, and other materials;
- interviewed USPTO officials, including system owners, the IT security and operations staff, and management;
- reviewed vulnerability scanning results conducted by USPTO during FY 2015;
- reviewed database vulnerability scanning results conducted by USPTO during the fourth quarter of FY 2016; and
- validated weak passwords by successfully logging in to the affected databases.

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
- IT Security Program Policy, U.S. Department of Commerce, introduced by the Chief Information Officer on September 12, 2014, and applicable Commerce Information Technology Requirements (CITR):
    - CITR-016, *Vulnerability Scanning and Patch Management*
    - CITR-017, *Security Configuration Checklist Program*
    - CITR-019, *Risk Management Framework (RMF)*
    - CITR-021, *Password Management*
    - CITR-024, *FedRAMP Applicability*
- *United States Patent and Trademark Office IT Security Handbook*, dated December 2015
- NIST Federal Information Processing Standards Publications:
    - 199, *Standards for Security Categorization of Federal Information and Information Systems*

  - 200, *Minimum Security Requirements for Federal Information and Information Systems*

- NIST Special Publications:
  - 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
  - 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans*

We conducted our field work from March 2016 to October 2016 at Department headquarters in Washington, DC, and USPTO offices in Alexandria, Virginia. We performed this audit under the authority of the Inspector General Act of 1978, as amended, 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: Descriptions of Selected Systems

DBS: The Database Services system consists of various types of databases that provide a database infrastructure to support USPTO's applications.

EUS: The Enterprise UNIX Services system consists of UNIX-based servers that provide a hosting platform to support USPTO applications.

PE2E: The Patent End-to-End is a next generation system that provides office action processing, workflow management, and role-based administration examination tools to track and manage the cases and view documents in text format.

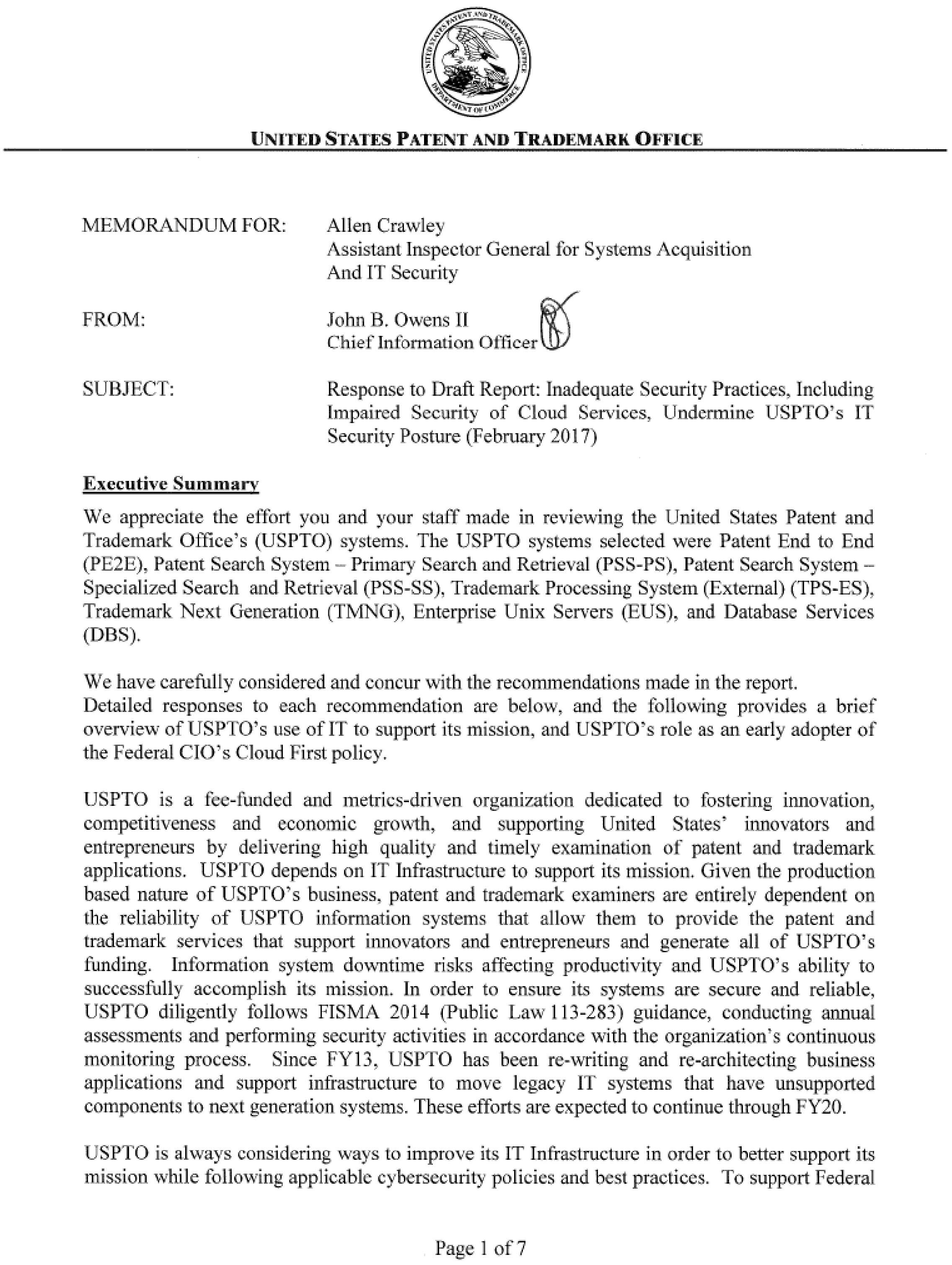
PSS-PS: The Patent Search System–Primary Search and Retrieval provides multiple means for querying U.S. and foreign patent data.

PSS-SS: The Patent Search System–Specialized Search provides access to highly specialized scientific or technology-based data such as annual submissions of nucleic and amino acid sequence or prior-art searching of polynucleotide and polypeptide sequences.

TMNG: The Trademark Next Generation system provides end-to-end support for processing of trademark applications. The system is used to submit or make changes to trademark applications, used by examining attorneys during the examination phase of an application, and enables consumers of published data in the official gazette to review information and search for items of interest.

TPS-ES: The Trademark Processing System–External Systems provides support to USPTO staff and public users through the trademark application process. The system allows users to complete and register a trademark domestically or internationally, provide support to trademark examining attorneys and the general public to search and retrieve design search codes, and assists Office of Trademark in sending and receiving data from the International Bureau, related to international applications that are being handled by the USPTO.

Appendix C: Agency Response



UNITED STATES PATENT AND TRADEMARK OFFICE

MEMORANDUM FOR: Allen Crawley
Assistant Inspector General for Systems Acquisition
And IT Security

FROM: John B. Owens II
Chief Information Officer

SUBJECT: Response to Draft Report: Inadequate Security Practices, Including Impaired Security of Cloud Services, Undermine USPTO's IT Security Posture (February 2017)

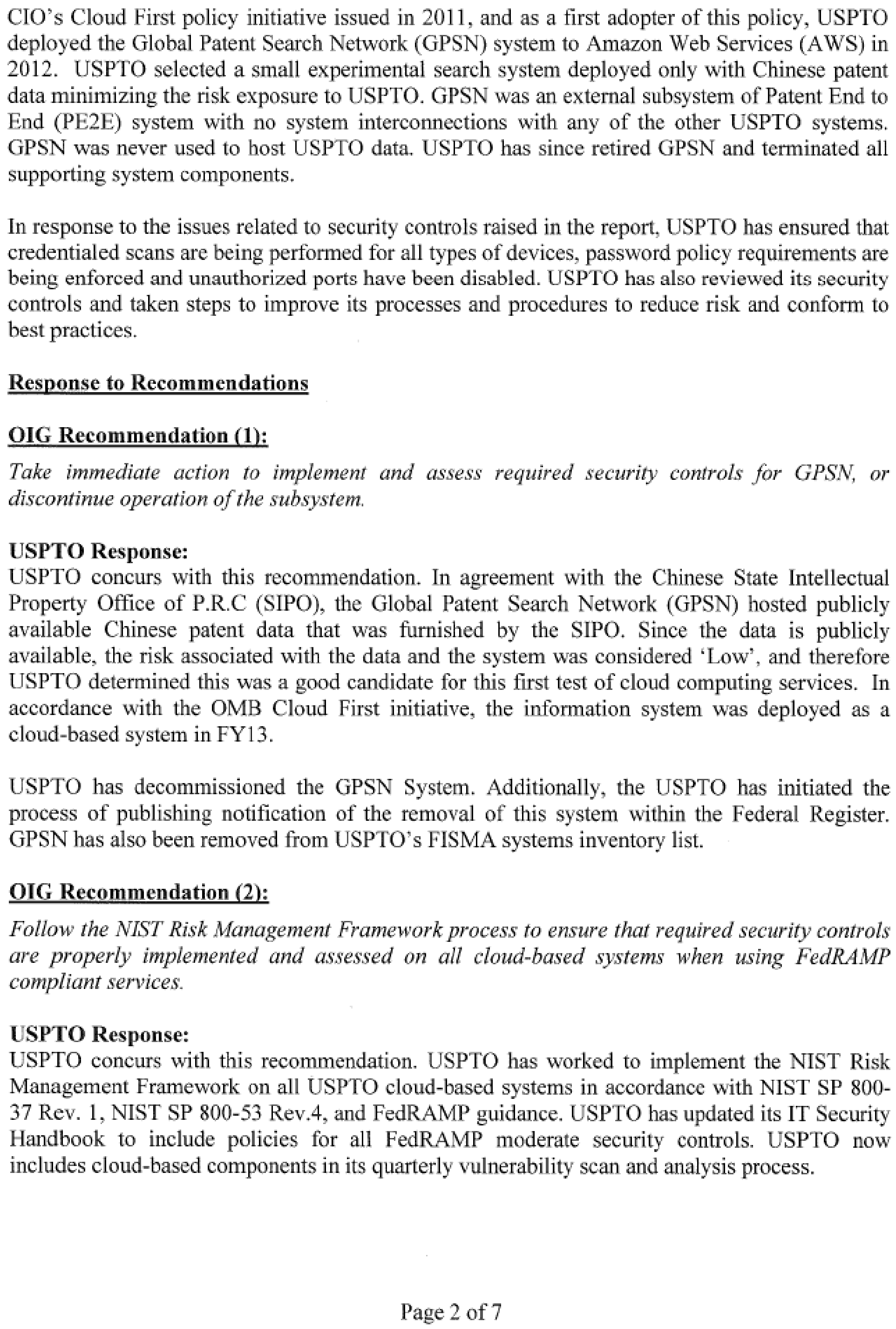
Executive Summary

We appreciate the effort you and your staff made in reviewing the United States Patent and Trademark Office's (USPTO) systems. The USPTO systems selected were Patent End to End (PE2E), Patent Search System – Primary Search and Retrieval (PSS-PS), Patent Search System – Specialized Search and Retrieval (PSS-SS), Trademark Processing System (External) (TPS-ES), Trademark Next Generation (TMNG), Enterprise Unix Servers (EUS), and Database Services (DBS).

We have carefully considered and concur with the recommendations made in the report. Detailed responses to each recommendation are below, and the following provides a brief overview of USPTO's use of IT to support its mission, and USPTO's role as an early adopter of the Federal CIO's Cloud First policy.

USPTO is a fee-funded and metrics-driven organization dedicated to fostering innovation, competitiveness and economic growth, and supporting United States' innovators and entrepreneurs by delivering high quality and timely examination of patent and trademark applications. USPTO depends on IT Infrastructure to support its mission. Given the production based nature of USPTO's business, patent and trademark examiners are entirely dependent on the reliability of USPTO information systems that allow them to provide the patent and trademark services that support innovators and entrepreneurs and generate all of USPTO's funding. Information system downtime risks affecting productivity and USPTO's ability to successfully accomplish its mission. In order to ensure its systems are secure and reliable, USPTO diligently follows FISMA 2014 (Public Law 113-283) guidance, conducting annual assessments and performing security activities in accordance with the organization's continuous monitoring process. Since FY13, USPTO has been re-writing and re-architecting business applications and support infrastructure to move legacy IT systems that have unsupported components to next generation systems. These efforts are expected to continue through FY20.

USPTO is always considering ways to improve its IT Infrastructure in order to better support its mission while following applicable cybersecurity policies and best practices. To support Federal



CIO's Cloud First policy initiative issued in 2011, and as a first adopter of this policy, USPTO deployed the Global Patent Search Network (GPSN) system to Amazon Web Services (AWS) in 2012. USPTO selected a small experimental search system deployed only with Chinese patent data minimizing the risk exposure to USPTO. GPSN was an external subsystem of Patent End to End (PE2E) system with no system interconnections with any of the other USPTO systems. GPSN was never used to host USPTO data. USPTO has since retired GPSN and terminated all supporting system components.

In response to the issues related to security controls raised in the report, USPTO has ensured that credentialed scans are being performed for all types of devices, password policy requirements are being enforced and unauthorized ports have been disabled. USPTO has also reviewed its security controls and taken steps to improve its processes and procedures to reduce risk and conform to best practices.

Response to Recommendations

OIG Recommendation (1):

Take immediate action to implement and assess required security controls for GPSN, or discontinue operation of the subsystem.

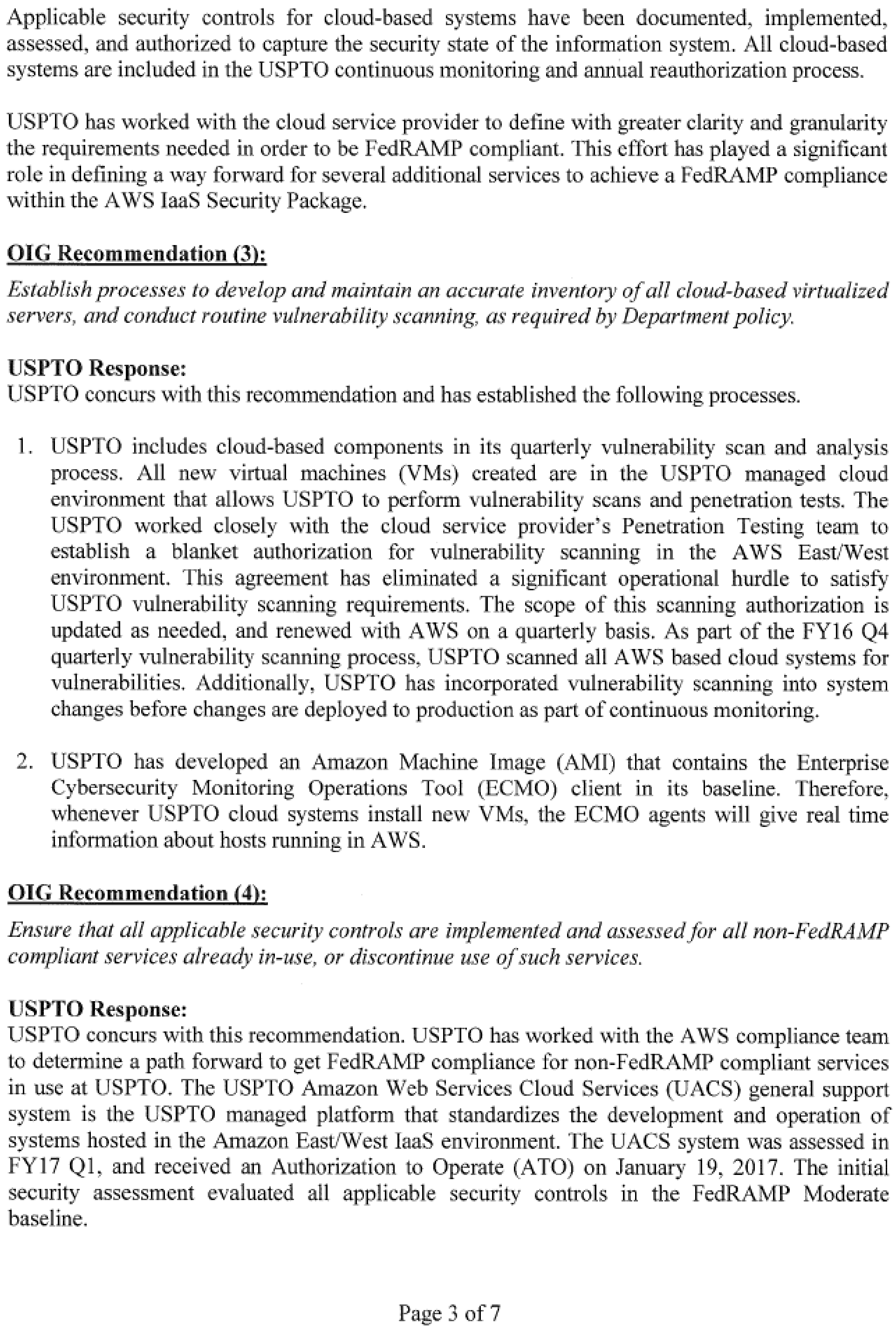
USPTO Response:
USPTO concurs with this recommendation. In agreement with the Chinese State Intellectual Property Office of P.R.C (SIPO), the Global Patent Search Network (GPSN) hosted publicly available Chinese patent data that was furnished by the SIPO. Since the data is publicly available, the risk associated with the data and the system was considered 'Low', and therefore USPTO determined this was a good candidate for this first test of cloud computing services. In accordance with the OMB Cloud First initiative, the information system was deployed as a cloud-based system in FY13.

USPTO has decommissioned the GPSN System. Additionally, the USPTO has initiated the process of publishing notification of the removal of this system within the Federal Register. GPSN has also been removed from USPTO's FISMA systems inventory list.

OIG Recommendation (2):

Follow the NIST Risk Management Framework process to ensure that required security controls are properly implemented and assessed on all cloud-based systems when using FedRAMP compliant services.

USPTO Response:
USPTO concurs with this recommendation. USPTO has worked to implement the NIST Risk Management Framework on all USPTO cloud-based systems in accordance with NIST SP 800-37 Rev. 1, NIST SP 800-53 Rev.4, and FedRAMP guidance. USPTO has updated its IT Security Handbook to include policies for all FedRAMP moderate security controls. USPTO now includes cloud-based components in its quarterly vulnerability scan and analysis process.



Applicable security controls for cloud-based systems have been documented, implemented, assessed, and authorized to capture the security state of the information system. All cloud-based systems are included in the USPTO continuous monitoring and annual reauthorization process.

USPTO has worked with the cloud service provider to define with greater clarity and granularity the requirements needed in order to be FedRAMP compliant. This effort has played a significant role in defining a way forward for several additional services to achieve a FedRAMP compliance within the AWS IaaS Security Package.

OIG Recommendation (3):

Establish processes to develop and maintain an accurate inventory of all cloud-based virtualized servers, and conduct routine vulnerability scanning, as required by Department policy.

USPTO Response:
USPTO concurs with this recommendation and has established the following processes.

1. USPTO includes cloud-based components in its quarterly vulnerability scan and analysis process. All new virtual machines (VMs) created are in the USPTO managed cloud environment that allows USPTO to perform vulnerability scans and penetration tests. The USPTO worked closely with the cloud service provider's Penetration Testing team to establish a blanket authorization for vulnerability scanning in the AWS East/West environment. This agreement has eliminated a significant operational hurdle to satisfy USPTO vulnerability scanning requirements. The scope of this scanning authorization is updated as needed, and renewed with AWS on a quarterly basis. As part of the FY16 Q4 quarterly vulnerability scanning process, USPTO scanned all AWS based cloud systems for vulnerabilities. Additionally, USPTO has incorporated vulnerability scanning into system changes before changes are deployed to production as part of continuous monitoring.

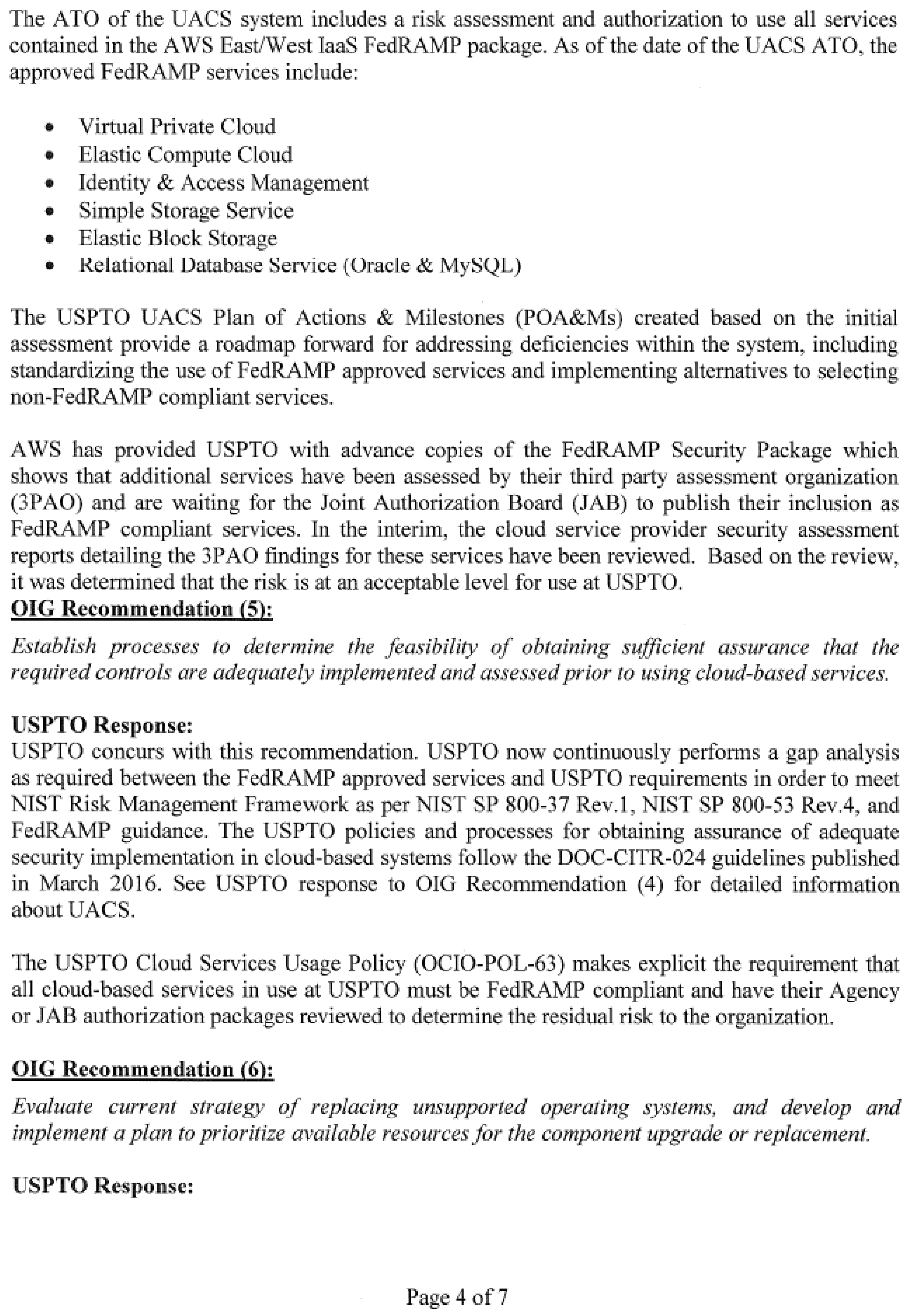
2. USPTO has developed an Amazon Machine Image (AMI) that contains the Enterprise Cybersecurity Monitoring Operations Tool (ECMO) client in its baseline. Therefore, whenever USPTO cloud systems install new VMs, the ECMO agents will give real time information about hosts running in AWS.

OIG Recommendation (4):

Ensure that all applicable security controls are implemented and assessed for all non-FedRAMP compliant services already in-use, or discontinue use of such services.

USPTO Response:
USPTO concurs with this recommendation. USPTO has worked with the AWS compliance team to determine a path forward to get FedRAMP compliance for non-FedRAMP compliant services in use at USPTO. The USPTO Amazon Web Services Cloud Services (UACS) general support system is the USPTO managed platform that standardizes the development and operation of systems hosted in the Amazon East/West IaaS environment. The UACS system was assessed in FY17 Q1, and received an Authorization to Operate (ATO) on January 19, 2017. The initial security assessment evaluated all applicable security controls in the FedRAMP Moderate baseline.

Page 3 of 7



The ATO of the UACS system includes a risk assessment and authorization to use all services contained in the AWS East/West IaaS FedRAMP package. As of the date of the UACS ATO, the approved FedRAMP services include:

- Virtual Private Cloud
- Elastic Compute Cloud
- Identity & Access Management
- Simple Storage Service
- Elastic Block Storage
- Relational Database Service (Oracle & MySQL)

The USPTO UACS Plan of Actions & Milestones (POA&Ms) created based on the initial assessment provide a roadmap forward for addressing deficiencies within the system, including standardizing the use of FedRAMP approved services and implementing alternatives to selecting non-FedRAMP compliant services.

AWS has provided USPTO with advance copies of the FedRAMP Security Package which shows that additional services have been assessed by their third party assessment organization (3PAO) and are waiting for the Joint Authorization Board (JAB) to publish their inclusion as FedRAMP compliant services. In the interim, the cloud service provider security assessment reports detailing the 3PAO findings for these services have been reviewed. Based on the review, it was determined that the risk is at an acceptable level for use at USPTO.

OIG Recommendation (5):

Establish processes to determine the feasibility of obtaining sufficient assurance that the required controls are adequately implemented and assessed prior to using cloud-based services.

USPTO Response:

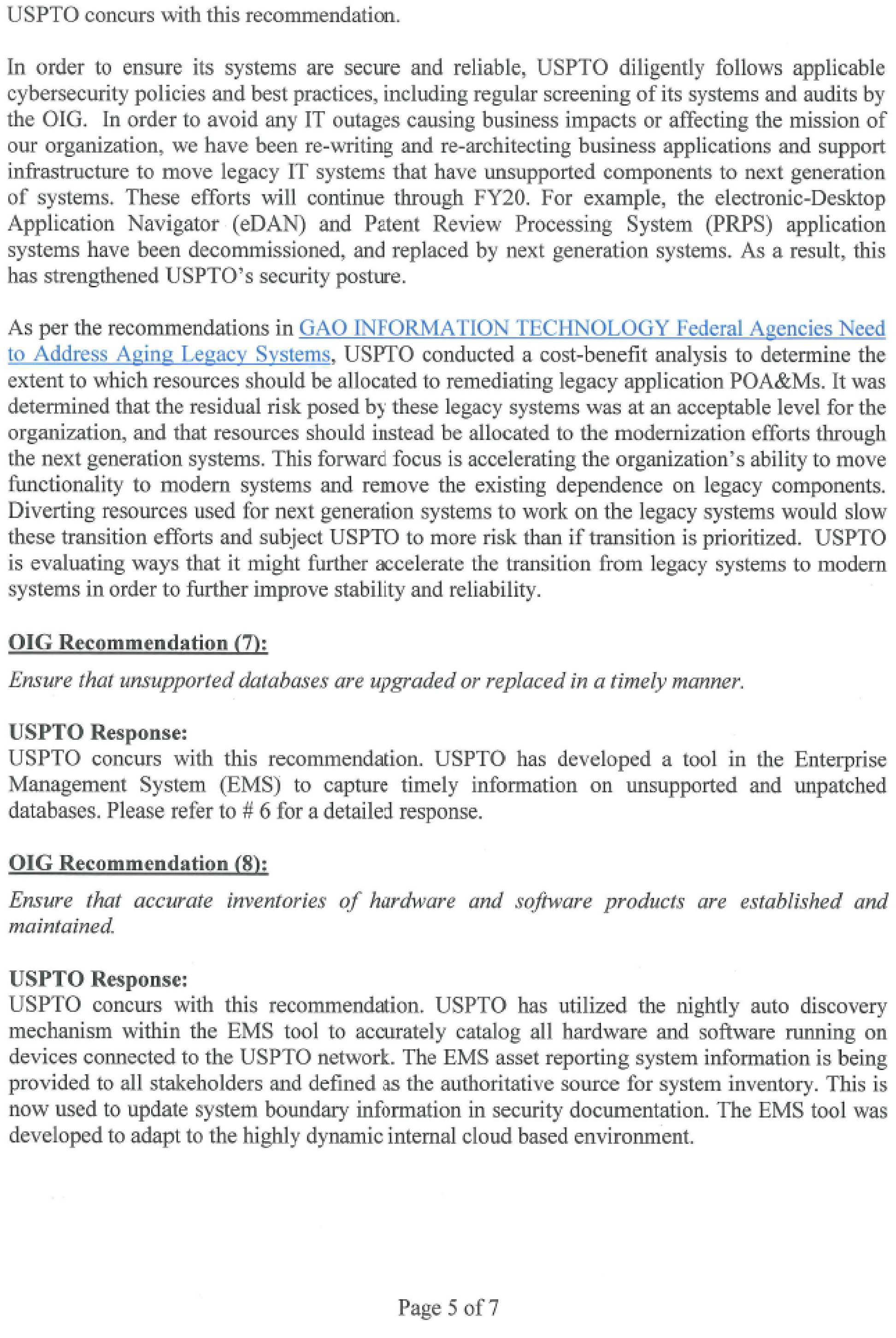
USPTO concurs with this recommendation. USPTO now continuously performs a gap analysis as required between the FedRAMP approved services and USPTO requirements in order to meet NIST Risk Management Framework as per NIST SP 800-37 Rev.1, NIST SP 800-53 Rev.4, and FedRAMP guidance. The USPTO policies and processes for obtaining assurance of adequate security implementation in cloud-based systems follow the DOC-CITR-024 guidelines published in March 2016. See USPTO response to OIG Recommendation (4) for detailed information about UACS.

The USPTO Cloud Services Usage Policy (OCIO-POL-63) makes explicit the requirement that all cloud-based services in use at USPTO must be FedRAMP compliant and have their Agency or JAB authorization packages reviewed to determine the residual risk to the organization.

OIG Recommendation (6):

Evaluate current strategy of replacing unsupported operating systems, and develop and implement a plan to prioritize available resources for the component upgrade or replacement.

USPTO Response:



USPTO concurs with this recommendation.

In order to ensure its systems are secure and reliable, USPTO diligently follows applicable cybersecurity policies and best practices, including regular screening of its systems and audits by the OIG. In order to avoid any IT outages causing business impacts or affecting the mission of our organization, we have been re-writing and re-architecting business applications and support infrastructure to move legacy IT systems that have unsupported components to next generation of systems. These efforts will continue through FY20. For example, the electronic-Desktop Application Navigator (eDAN) and Patent Review Processing System (PRPS) application systems have been decommissioned, and replaced by next generation systems. As a result, this has strengthened USPTO's security posture.

As per the recommendations in GAO INFORMATION TECHNOLOGY Federal Agencies Need to Address Aging Legacy Systems, USPTO conducted a cost-benefit analysis to determine the extent to which resources should be allocated to remediating legacy application POA&Ms. It was determined that the residual risk posed by these legacy systems was at an acceptable level for the organization, and that resources should instead be allocated to the modernization efforts through the next generation systems. This forward focus is accelerating the organization's ability to move functionality to modern systems and remove the existing dependence on legacy components. Diverting resources used for next generation systems to work on the legacy systems would slow these transition efforts and subject USPTO to more risk than if transition is prioritized. USPTO is evaluating ways that it might further accelerate the transition from legacy systems to modern systems in order to further improve stability and reliability.

OIG Recommendation (7):

Ensure that unsupported databases are upgraded or replaced in a timely manner.

USPTO Response:
USPTO concurs with this recommendation. USPTO has developed a tool in the Enterprise Management System (EMS) to capture timely information on unsupported and unpatched databases. Please refer to # 6 for a detailed response.

OIG Recommendation (8):

Ensure that accurate inventories of hardware and software products are established and maintained.

USPTO Response:
USPTO concurs with this recommendation. USPTO has utilized the nightly auto discovery mechanism within the EMS tool to accurately catalog all hardware and software running on devices connected to the USPTO network. The EMS asset reporting system information is being provided to all stakeholders and defined as the authoritative source for system inventory. This is now used to update system boundary information in security documentation. The EMS tool was developed to adapt to the highly dynamic internal cloud based environment.

OIG Recommendation (9):

Establish a process to ensure effective coordination between the Cybersecurity Division and operation teams to timely share critical security information such as credentials and vulnerability scanning reports.

USPTO Response:
USPTO concurs with this recommendation. USPTO has taken action and continues to ensure that credential checks are performed prior to scanning all types of device targets. These checks will test and see if the connections using the scanning credentials are successful and proper privileges have been assigned. USPTO will update its Software Development Lifecycle plan or create a communications plan that will ensure more collaboration between various groups within the OCIO.

OIG Recommendation (10):

Establish vulnerability scanning procedures that require credentialed scanning of all system components as required by Department and USPTO policies.

USPTO Response:
USPTO concurs with this recommendation. USPTO is actively working on improving and maturing the vulnerability and compliance scanning program. The following steps have been taken to improve scan coverage:

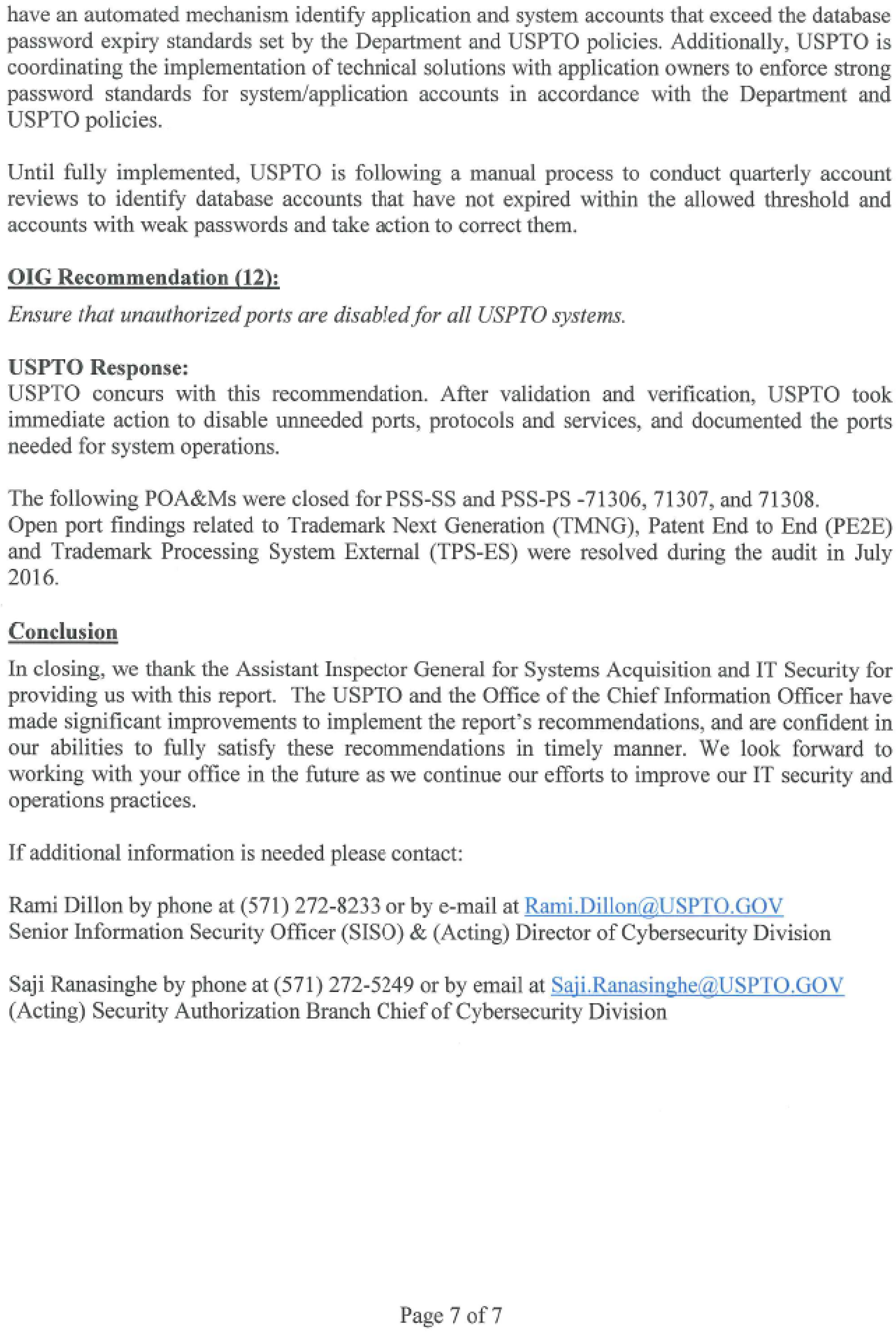
1. Increased Number of Licenses for scanning tools (i.e. HP WebInspect)
2. Migrated Web URL scanning tool from laptops to dedicated VM servers
3. Migrated Database scanning tool from scanning laptops to dedicated VM servers
4. Upgraded Database scanning tool to an enterprise solution that allows scanning more database targets
5. Plans to add Tenable Security Center sensors to network segments that are not visible to Tenable Nessus Security Center

USPTO will also update its IT Security Handbook and Risk Assessment (RA) procedures to address the findings in the recommendation. Scans for all applicable systems, database instances, and web applications will be performed each quarter. USPTO's new asset reporting mechanism will serve to provide data on all components in the system boundaries. This is now used to update the security documentation.

OIG Recommendation (11):

Ensure that passwords for user and DBA database accounts meet the standards set by Department and USPTO policies.

USPTO Response:
USPTO concurs with this recommendation. USPTO uses predefined profiles for actual people accounts that follow USPTO policy. However, application and system accounts are placed in a different profile that explicitly does not follow user password policy due to risk of interruption of services crashing an application. USPTO is working towards implementing technical controls to



have an automated mechanism identify application and system accounts that exceed the database password expiry standards set by the Department and USPTO policies. Additionally, USPTO is coordinating the implementation of technical solutions with application owners to enforce strong password standards for system/application accounts in accordance with the Department and USPTO policies.

Until fully implemented, USPTO is following a manual process to conduct quarterly account reviews to identify database accounts that have not expired within the allowed threshold and accounts with weak passwords and take action to correct them.

OIG Recommendation (12):

Ensure that unauthorized ports are disabled for all USPTO systems.

USPTO Response:
USPTO concurs with this recommendation. After validation and verification, USPTO took immediate action to disable unneeded ports, protocols and services, and documented the ports needed for system operations.

The following POA&Ms were closed for PSS-SS and PSS-PS -71306, 71307, and 71308.
Open port findings related to Trademark Next Generation (TMNG), Patent End to End (PE2E) and Trademark Processing System External (TPS-ES) were resolved during the audit in July 2016.

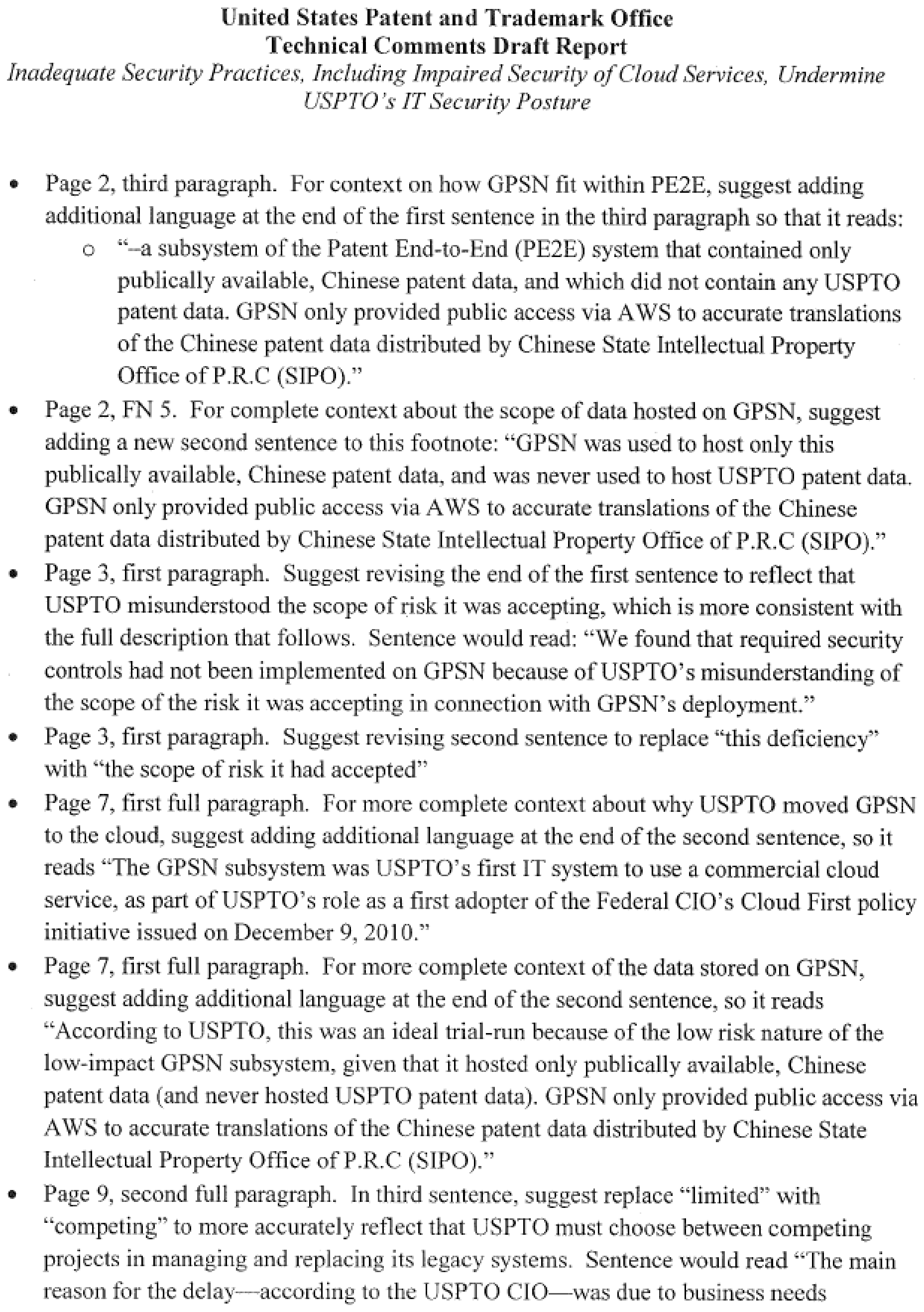
Conclusion

In closing, we thank the Assistant Inspector General for Systems Acquisition and IT Security for providing us with this report. The USPTO and the Office of the Chief Information Officer have made significant improvements to implement the report's recommendations, and are confident in our abilities to fully satisfy these recommendations in 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:

Rami Dillon by phone at (571) 272-8233 or by e-mail at Rami.Dillon@USPTO.GOV
Senior Information Security Officer (SISO) & (Acting) Director of Cybersecurity Division

Saji Ranasinghe by phone at (571) 272-5249 or by email at Saji.Ranasinghe@USPTO.GOV
(Acting) Security Authorization Branch Chief of Cybersecurity Division



United States Patent and Trademark Office
Technical Comments Draft Report
Inadequate Security Practices, Including Impaired Security of Cloud Services, Undermine USPTO's IT Security Posture

- Page 2, third paragraph. For context on how GPSN fit within PE2E, suggest adding additional language at the end of the first sentence in the third paragraph so that it reads:
    - "–a subsystem of the Patent End-to-End (PE2E) system that contained only publically available, Chinese patent data, and which did not contain any USPTO patent data. GPSN only provided public access via AWS to accurate translations of the Chinese patent data distributed by Chinese State Intellectual Property Office of P.R.C (SIPO)."
- Page 2, FN 5. For complete context about the scope of data hosted on GPSN, suggest adding a new second sentence to this footnote: "GPSN was used to host only this publically available, Chinese patent data, and was never used to host USPTO patent data. GPSN only provided public access via AWS to accurate translations of the Chinese patent data distributed by Chinese State Intellectual Property Office of P.R.C (SIPO)."
- Page 3, first paragraph. Suggest revising the end of the first sentence to reflect that USPTO misunderstood the scope of risk it was accepting, which is more consistent with the full description that follows. Sentence would read: "We found that required security controls had not been implemented on GPSN because of USPTO's misunderstanding of the scope of the risk it was accepting in connection with GPSN's deployment."
- Page 3, first paragraph. Suggest revising second sentence to replace "this deficiency" with "the scope of risk it had accepted"
- Page 7, first full paragraph. For more complete context about why USPTO moved GPSN to the cloud, suggest adding additional language at the end of the second sentence, so it reads "The GPSN subsystem was USPTO's first IT system to use a commercial cloud service, as part of USPTO's role as a first adopter of the Federal CIO's Cloud First policy initiative issued on December 9, 2010."
- Page 7, first full paragraph. For more complete context of the data stored on GPSN, suggest adding additional language at the end of the second sentence, so it reads "According to USPTO, this was an ideal trial-run because of the low risk nature of the low-impact GPSN subsystem, given that it hosted only publically available, Chinese patent data (and never hosted USPTO patent data). GPSN only provided public access via AWS to accurate translations of the Chinese patent data distributed by Chinese State Intellectual Property Office of P.R.C (SIPO)."
- Page 9, second full paragraph. In third sentence, suggest replace "limited" with "competing" to more accurately reflect that USPTO must choose between competing projects in managing and replacing its legacy systems. Sentence would read "The main reason for the delay—according to the USPTO CIO—was due to business needs

requiring the legacy systems continued operation and the competing resources USPTO has to commit to the migration effort."