Deficiencies in USPTO's Backup and Restoration Process Could Delay Recovery of Critical Applications in the Event of a System Failure and Adversely Affect Its Mission

FINAL REPORT NO. OIG-20-030-A
JUNE 16, 2020

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 16, 2020

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: *Deficiencies in USPTO's Backup and Restoration Process Could Delay Recovery of Critical Applications in the Event of a System Failure and Adversely Affect Its Mission*
Final Report No. OIG-20-030-A

Attached for your review is our final report on the audit of the U.S. Patent and Trademark Office's (USPTO's) Patent Capture and Application Processing System (PCAPS). Our objective was to determine whether USPTO has adequate data recovery and contingency plans in place to ensure operational availability of PCAPS.

We found that

I. USPTO has no assurance that it can restore critical applications in the event of system failure, and

II. USPTO's continued delay in updating legacy systems rendered a $4 million-per-year alternate processing site inadequate and impractical.

On May 22, 2020, we received USPTO's response to our draft report. In response to our draft report, USPTO concurred with all of our recommendations and described actions it has taken, or will take, to address them. USPTO's formal response is included within the final report as appendix C.

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. This 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 our 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.

Attachment

cc: André Mendes, Acting Chief Information Officer
Laura Peter, Deputy Under Secretary of Commerce for Intellectual Property and Deputy Director, USPTO
Jamie Holcombe, Chief Information Officer, USPTO
Welton Lloyd, Jr., Audit Liaison, USPTO
Mohamed Ahmed, Assistant Audit Liaison, USPTO
Jay Hoffman, Chief Financial Officer, USPTO
Sean Mildrew, Deputy Chief Financial Officer and Audit Resolution Officer, USPTO
Nicholas Matich, Acting General Counsel, USPTO
Joselyn Bingham, Audit Liaison, OCIO
Jason Schwartz, IT Security Audit Support, OCIO
MaryAnn Mausser, Audit Liaison, Office of the Secretary

Report in Brief

June 16, 2020

Background

The U.S. Department of Commerce and its bureaus are required to follow federal laws to secure information technology (IT) systems through the use of cost-effective 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." USPTO relies heavily on IT infrastructure, systems, and applications to achieve its mission.

One critical component of USPTO IT infrastructure is the Patent Capture and Application Processing System (PCAPS). PCAPS is a legacy information system initially deployed in the early 1970s that supports patent application capture, processing, reporting, and retrieval and display. It is comprised of multiple software applications including the Patent Application Locating and Monitoring (PALM) system. PALM is a critical system that tracks every step of the patent process and interfaces with more than 20 USPTO software applications.

Why We Did This Review

Our audit objective was to determine whether USPTO has adequate data recovery and contingency plans in place to ensure operational availability of PCAPS. This audit was conducted as a result of a prolonged outage that took place with PCAPS in August 2018.

U.S. PATENT AND TRADEMARK OFFICE

Deficiencies in USPTO's Backup and Restoration Process Could Delay Recovery of Critical Applications in the Event of a System Failure and Adversely Affect Its Mission

OIG-20-030-A

WHAT WE FOUND

We found that USPTO did not have adequate data recovery and contingency plans in place to ensure operational availability of PCAPS. Specifically, USPTO has no assurance that it can restore critical applications in the event of a system failure. We noted major deficiencies in its data recovery and contingency planning processes, including incomplete contingency documentation; inadequate contingency plan testing and participation; and poorly coordinated backup processes and monitoring.

Additionally, we found that USPTO's $4 million-per-year alternate processing site is underutilized and does not provide the documented functionality, including timely resumption of critical applications in an event of system disruption. This is due, in part, to USPTO's continued postponement of replacing or upgrading functionally-limited legacy systems—an undertaking planned since 2012.

These identified deficiencies adversely affect USPTO's ability to carry out its mission in the event of disruption, failure, or unavailability of PCAPS.

WHAT WE RECOMMEND

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the U.S. Patent and Trademark Office direct the Chief Information Officer to do the following:

1. Implement recommendations outlined in NIST SP 800-34 to ensure that all contingency planning documentation contains the necessary components, including, but not limited to, recovery objectives.
2. Establish a documented process that ensures contingency plan testing includes functional testing that entails simulations of actual system disruption or failure, and that all required participants are involved with contingency plan testing.
3. Ensure that appropriate backup logs are delivered to the CIO Command Center and backup failures are flagged for review while also establishing a process to alert appropriate personnel who can promptly rectify any failures.
4. Make a determination whether the $4 million in potential monetary benefits that we have identified in this report that is currently allocated for the Boyers alternate site can be used more efficiently.
5. Establish a detailed plan for the replacement of legacy systems and software applications, including milestones and deadlines, and enforce the plan in a manner that holds appropriate personnel accountable.

Contents

Cover: Herbert C. Hoover Building main entrance at 14th Street Northwest in Washington, DC. Completed in 1932, the building is named after the former Secretary of Commerce and 31st President of the United States.

Introduction

The U.S. Department of Commerce and its bureaus are required to follow federal laws to secure information technology (IT) systems[1] through the use of cost-effective 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."[2] USPTO relies heavily on IT infrastructure, systems, and applications to achieve its mission.

One critical component of USPTO IT infrastructure is the Patent Capture and Application Processing System (PCAPS).[3] PCAPS is a legacy information system[4] initially deployed in the early 1970s that supports patent application capture, processing, reporting, and retrieval and display. It is comprised of multiple software applications including the Patent Application Locating and Monitoring (PALM) system. PALM is a critical system that tracks every step of the patent process and interfaces with more than 20 USPTO software applications.

USPTO was left significantly limited in its ability to carry out its mission during August 2018 when the PALM system went off-line for 9 days (August 15–23). USPTO did not restore the system in a timely manner resulting in patent examiners being unable to perform some of their job functions, such as maintaining time, activity, and docket records. The outage also caused disruptions to USPTO customers who were unable to manage current, or file new, patent applications. This incident illustrated the necessity of effective data recovery and contingency planning to ensure availability of USPTO's mission-critical systems.

---

[1] Federal Information Security Modernization Act of 2014, Pub. L. No. 113–283 (Dec. 18, 2014), amending the Federal Information Security Management Act of 2002, Pub. L. No. 107–347 (Dec. 17, 2002).

[2] U.S. Department of Commerce. *U.S. Patent and Trademark Office* [online]. https://www.commerce.gov/bureaus-and-offices/uspto (accessed December 31, 2019).

[3] PCAPS is divided into two systems for Federal Information Security Modernization Act (FISMA) compliance purposes: PCAPS Initial Processing (PCAPS-IP) and PCAPS Examination Support (PCAPS-ES).

[4] In the context of IT, *legacy systems* are outdated computer systems and software applications.

Objective, Findings, and Recommendations

Our audit objective was to determine whether USPTO has adequate data recovery and contingency plans in place to ensure operational availability of PCAPS. This audit was conducted as a result of a prolonged outage that took place with PCAPS in August 2018. Our audit scope included data recovery and contingency plan processes, procedures, and activities of PCAPS. Appendix A provides a more detailed description of our audit objective, scope, and methodology.

We found that USPTO did not have adequate data recovery and contingency plans in place to ensure operational availability of PCAPS. Specifically, USPTO has no assurance that it can restore critical applications in the event of a system failure (see finding I). We noted major deficiencies in its data recovery and contingency planning processes, including incomplete contingency documentation; inadequate contingency plan testing and participation; and poorly coordinated backup processes and monitoring.

Additionally, we found that USPTO's $4 million-per-year alternate processing site is underutilized and does not provide the documented functionality, including timely resumption of critical applications in an event of system disruption. This is due, in part, to USPTO's continued postponement of replacing or upgrading functionally-limited legacy systems—an undertaking planned since 2012. (See finding II, recommendation 4, and appendix B for further information regarding the potential monetary benefits identified in this report.)

These identified deficiencies adversely affect USPTO's ability to carry out its mission in the event of disruption, failure, or unavailability of PCAPS.

I. USPTO Has No Assurance That It Can Restore Critical Applications in the Event of System Failure

We analyzed USPTO contingency plan testing and backup and restoration processes and found them inadequate to assure proper restoration of PCAPS. Specifically, we found that (1) contingency plans did not define recovery objectives, (2) contingency plan tests were not adequate, and (3) USPTO lacked coordination and monitoring of backup processes.

A. Contingency plans did not define recovery objectives

A contingency plan is required for all federal information systems. It addresses disaster response, backup operations, and post-disaster recovery in an effort to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation. As required by National Institute of Standards and Technology (NIST) standards, one of the first steps when developing a contingency plan is to perform a business impact analysis (BIA).[5] A BIA is an analysis of an information system's

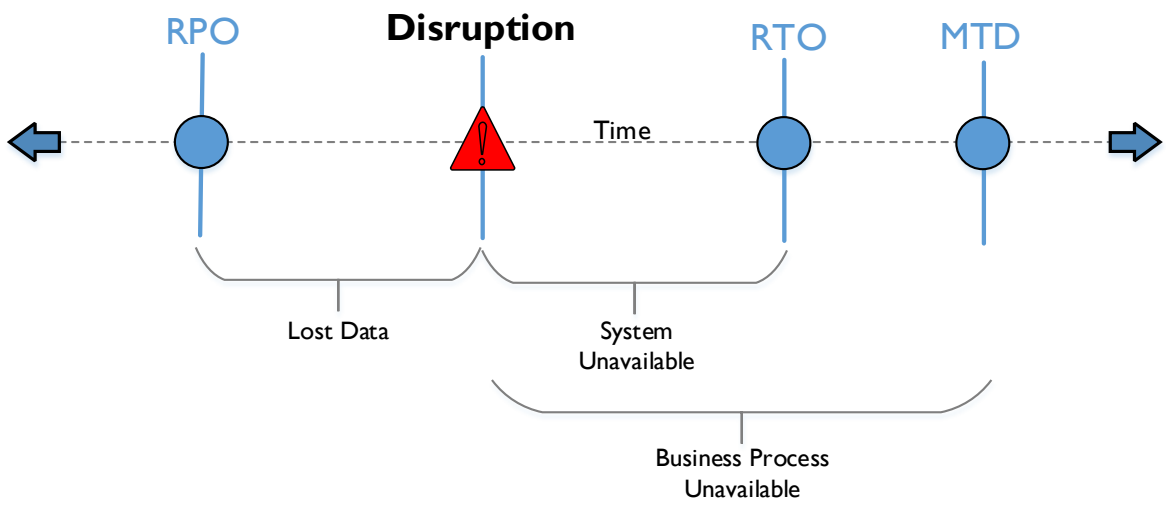
[5] *See* (1) U.S. Department of Commerce National Institute of Standards and Technology, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations: CP-2 (Contingency Plan)*, NIST Special Publication (SP) 800-53, Rev. 4. Gaithersburg, MD: DOC NIST;

requirements, functions, and interdependencies used to characterize contingency requirements and priorities in the event of significant disruption. In summary, BIAs are the originating product from which contingency determinations and decisions are made. A key component of a BIA is the determination of recovery objectives, which includes the following:

- **Maximum tolerable downtime (MTD)** – the total amount of time that is acceptable for a business process outage or disruption.
- **Recovery time objective (RTO)** – the maximum amount of time that a system can remain unavailable before there is an unacceptable impact on other system resources, supported mission or business processes, or the MTD.
- **Recovery point objective (RPO)** – the point in time, prior to a system disruption or outage, to which mission or business process data can be recovered after an outage.

The relationship among these different terms is illustrated in figure 1.

Figure 1. Recovery Objectives Timeline



Source: Created by OIG based on information in NIST SP 800-34

Therefore, it is crucial to first define recovery objectives to determine resource and personnel requirements and to inform appropriate policies and procedures. For example, defining an RPO for a system will determine what methods of backup are acceptable and how often they need to be performed. Similarly, defining an RTO and

(2) DOC NIST, May 2010. *Contingency Planning Guide for Federal Information Systems*, NIST SP 800-34, Rev. 1. Gaithersburg, MD: DOC NIST, chapter 3;
(3) DOC NIST, February 2004. *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 199. Gaithersburg, MD: DOC NIST; and
(4) DOC NIST, March 2006. *Minimum Security Requirements for Federal Information and Information Systems*, FIPS PUB 200. Gaithersburg, MD: DOC NIST.

MTD for a system helps determine desired capabilities as it relates to contingency and recovery activities, and creates a baseline against which contingency plan testing results can be compared.

We found that USPTO contingency planning documentation did not define any recovery objectives—and that, instead, a cascade of documentation referencing existed. For example, regarding recovery objectives, system security plans and common controls documentation referred to contingency plans that, in turn, referred to business resumption plans, which evidently do not exist. We requested the referenced business resumption plans on multiple occasions from USPTO, and those plans were never provided. Instead, we received an aggregation of MTDs for certain applications as defined by different USPTO component offices. The MTDs for each application varied depending on which component office was providing feedback. For example, a single application may have a 1-month MTD for office 1, 2-week MTD for office 2, and a 1-hour MTD for office 3. This survey collection of component offices' requirements is an appropriate start, but it is just that—a start. The next step USPTO must take would be to leverage these survey results to define official recovery objectives that reflect the needs of the organization.

Without defined recovery objectives, USPTO personnel do not know either how much downtime is acceptable or how much money should be allocated for recovery and contingency capabilities. Additionally, it is difficult for the organization to judge the success or failure of contingency plan tests without defined recovery objectives. It is incumbent upon executive leadership to determine these recovery objectives to enable informed policies and procedures to guide necessary resource expenditures.

B. Contingency plan tests were not adequate

All federal information systems with a moderate-impact level[6]—such as PCAPS—are required to have a contingency plan to be properly tested annually. According to NIST's *Contingency Planning Guide for Federal Information Systems*[7] and USPTO IT security policy, a functional exercise should be conducted for all moderate-impact systems. A functional exercise is defined as a "[s]imulation of a disruption with a system recovery component such as backup tape restoration or server recovery."[8] USPTO contingency plan testing procedures also require several participants to be involved in the testing, such as the information system owner and its point of contact, information system security officer, administrators from the operating systems operations section (OSOS) and database services (DBS) teams, and a service desk representative.[9]

---

[6] NIST identifies potential impacts on organizations should there be a breach of security, and classifies those impacts into three defined categories: low-, moderate-, or high-impact. *See* FIPS PUB 199, sections 2–3.

[7] NIST SP 800-34, 30.

[8] *Ibid*, 31.

[9] DOC U.S. Patent and Trademark Office, March 26, 2018. *United States Patent and Trademark Office IT Security Handbook*, Ver. 5.3. Alexandria, VA: DOC USPTO.

We reviewed USPTO's documentation and found that it conducted contingency plan testing on an annual basis. However, several USPTO officials stated that functional exercises were limited. For example, instead of restoring an entire server or database, only a single file was restored for the functional exercise component of the test. Restoring a single file does not provide assurance that the tested contingency plan and recovery functions would be sufficient in the event of a real information system disruption or failure. We also found that only two of the required six personnel participated in the testing process.

According to USPTO officials, the tests were limited because USPTO lacked a testing environment where fully functional tests can be executed without significant disruption to operations. For example, in the case of the PALM database, because of its legacy design, it cannot be replicated to USPTO's alternate processing site in Boyers, Pennsylvania, where it could be fully tested.[10] The alternative approach in this case is to perform the tests on the production environment, which management is reluctant to support because of the risk associated with negatively affecting USPTO business functions. Undertaking a fully functional test on the production environment would mean halting all business functions until the test is complete, which could last for hours or days if the process deviates from USPTO's intended plan.

Inadequate testing resulted in USPTO having no assurance that critical applications could be restored in a timely manner, as was illustrated during the PALM outage in August 2018. In fact, during the August 2018 event, it was the failure of a backup that caused USPTO's prolonged 9-day recovery and reconstitution of critical data. This delay disrupted the critical mission of granting patents. According to patent examination personnel, an outage lasting only 1 day adversely affects their ability to execute their job functions.

Contingency plans play an important role in the overall management of USPTO's information systems and, ultimately, the ability of USPTO to execute its mission. These plans should be maintained in a state of readiness, including having them properly tested with required and appropriate personnel to ensure their operability.

C. USPTO lacked coordination and monitoring of backup processes

PCAPS primarily uses Oracle™ for its database solution, which is deployed using different methods—namely, Oracle Single Instance (SI) and Oracle Real Application Clusters (RAC). PCAPS contingency plans require all information systems, including database systems, to be backed up regularly.[11] As illustrated in figure 2, the backup process varies depending on the deployment method. With Oracle SI, the DBS team generates local backups (figure 2, label 1) that are then pulled and archived by the OSOS

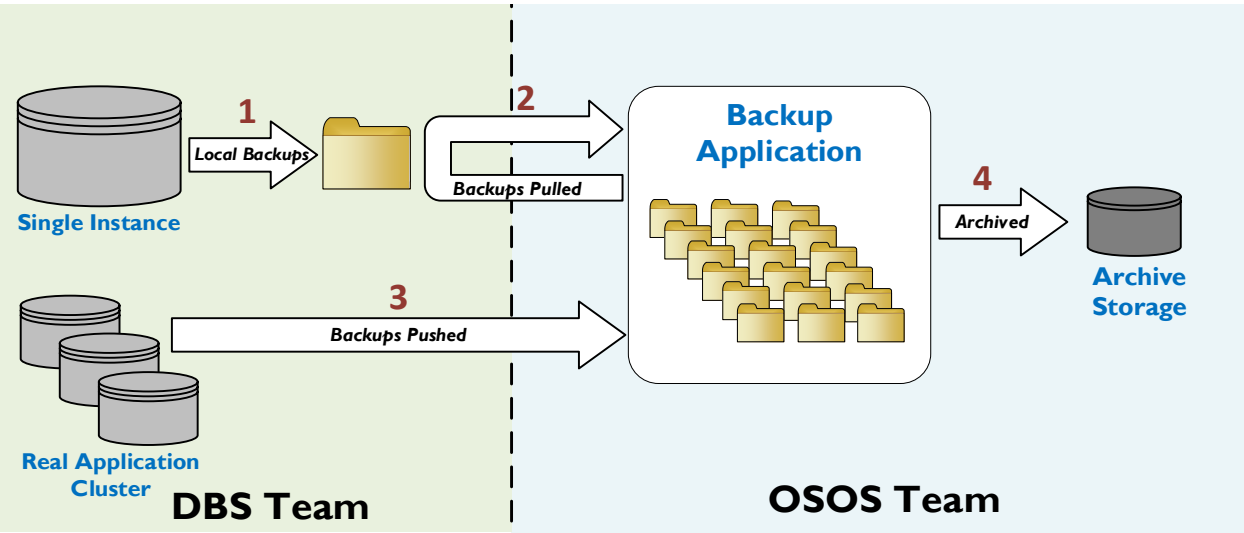
[10] Finding II of this report provides more details regarding the alternate processing and legacy systems.

[11] *See* (1) DOC USPTO, January 8, 2019. *Patent Capture and Processing System-Initial Processing (PCAPS-IP): Information System Contingency Plan (ISCP)*, Ver. 3.2. Alexandria, VA: DOC USPTO, 19; and
(2) DOC USPTO, February 19, 2019. *Patent Capture and Application Processing System-Examination Support (PCAPS-ES): Information System Contingency Plan (ISCP)*, Ver. 5.1. Alexandria, VA: DOC USPTO, 24.

team (figure 2, label 2). With Oracle RAC, the DBS team pushes the backups directly to the OSOS team for archiving (figure 2, label 3). The OSOS team ultimately archives the backups it receives via deduplication storage devices or physical tapes (figure 2, label 4).

We found that each team has visibility of only their own processes and would not be aware if a process of the other team has failed. For example, if a local backup initiated by the DBS team were to fail (figure 2, label 1), the OSOS team would not be aware and would back up outdated or corrupted data (figure 2, label 2). Centralized monitoring of backup logs can help mitigate this visibility issue. In fact, USPTO policy requires such logs to be sent to the CIO Command Center (C3) so failures can be flagged for examination and, ultimately, remediated.[12] With the assistance of USPTO, we searched the centralized log location at C3 and did not find logs for backup operations.

Figure 2. USPTO PALM Database Backup Process



Source: OIG analysis

This lack of coordination and monitoring contributed to the prolonged PALM outage in August 2018, where 3 weeks of preceding backups were incomplete. If those backup failures had been identified, it was likely the underlying issue would have been quickly rectified, thereby ensuring complete and usable backups in the event of the outage. Better oversight and monitoring of the backup process, as well as better coordination between USPTO teams, is needed to ensure backup processes are successfully executed.

[12] DOC USPTO, September 13, 2012. *CIO Command Center Policy OCIO-POL-45*, Ver. 2.0. Alexandria, VA: DOC USPTO, 5.

II. USPTO's Continued Delay in Updating Legacy Systems Rendered a $4 Million-Per-Year Alternate Processing Site Inadequate and Impractical

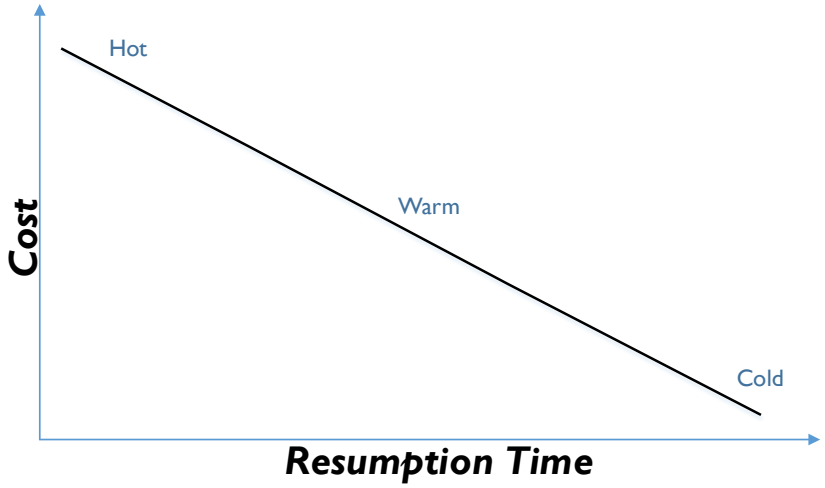
Alternate processing sites are those that are located in different geographical regions than primary processing sites, with the purpose of providing continuity of operations in the event that the primary processing site is not available. Resources and requirements are commensurately allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission or business functions despite disruption, compromise, or failure of organizational information systems. Alternate processing sites vary in capability and cost depending on those requirements. NIST generally categorizes the three deployment models as follows:[13]

- **Hot site** – a fully operational facility equipped with hardware and software, to be used in the event of an information system disruption. Recovery to a hot site takes minutes to hours.
- **Warm site** – a facility that is partially equipped to support relocating or reestablishing information systems from a primary facility. Recovery to a warm site takes several hours to several days.
- **Cold site** – a backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement equipment in the event that users have to move from their main computing location to an alternate site. Recovery to a cold site takes several days to several weeks.

Variations or hybrid mixtures of these deployment models can be leveraged to procure the appropriate capabilities. Core requirements should be evaluated in order to establish the most effective solution. As illustrated in figure 3, cost of an alternate processing site has a positive relationship with the capabilities, while resumption time at an alternate processing site has a negative relationship. In summary, an organization can resume operations more quickly at a hot site than a cold site, but at additional cost.

[13] NIST Information Technology Laboratory Computer Security Resource Center. *Glossary* [online]. https://csrc.nist.gov/glossary (accessed February 12, 2020).

Figure 3. Alternate Processing Site Deployment Model Characteristics



Source: Created by OIG based on information in NIST SP 800-34

USPTO IT security policy requires the establishment of an alternate processing site that enables resumption of all critical information system operations for essential mission and business functions within the recovery objective timeframes when primary processing capabilities are unavailable.[14] Equipment and supplies required to transfer and resume operations must be available at the alternate processing site to support systems transfer or resumption in accordance with defined recovery objectives. As discussed in finding I of this report, USPTO has not defined recovery objectives.

USPTO established an alternate site at the Iron Mountain facility in Boyers, Pennsylvania, in 2013. With an annual average cost of more than $4 million,[15] the 10 thousand-square-foot site comprises a data center, working space with 10 cubicles, conference room, small exercise room, and living quarters with four bedrooms, two bathrooms, and a fully-furnished kitchen. Despite the substantial cost of the Boyers facility, we observed a significant underutilization of the site. According to multiple UPSTO officials, utilization of the site is between 10 and 30 percent. Much of the data center is unoccupied space. Of the equipment that is installed, roughly half of it is not being utilized. For example, there was a large tape machine in the data center that was purchased at a cost of $500,000 that was never used and is slated to be decommissioned.

This significant underutilization of the alternate site is due, in most part, to the technical limitations of legacy systems. The Boyers facility was originally planned to be a fully functional hot site by 2016. This deployment plan, however, was contingent on the replacement of USPTO legacy systems, some of which were originally deployed in the 1970s. For technical reasons, legacy systems cannot be deployed at alternate sites in a

[14] *United States Patent and Trademark Office IT Security Handbook*.

[15] This amount includes rent and utilities.

timely manner.[16] It would take months to deploy all legacy systems to an alternate site, according to USPTO officials who would be responsible for such an undertaking.

Legacy systems have continued to present major challenges on USPTO's IT security front, and USPTO has consistently demonstrated its ineffectiveness in prioritizing and remediating this problem. We have reported on legacy system issues multiple times in the past,[17] but USPTO continues to push replacement or modernization dates further into the future. In fact, USPTO has had plans to replace legacy systems since 2012; 7 years later, the target date is 2021. According to USPTO officials, only 10 percent (3 out of 30) of legacy software applications within PCAPS have been retired.

The functionality delivered by the alternate site is more akin to that of a cold site implementation, not a hot site. Even though the data and application files of legacy systems are copied to Boyers, they cannot be used to bring the software applications to an operational state at the alternate site. Our observations and the prolonged PALM outage in August 2018 were in direct conflict with USPTO contingency documentation describing the alternate site as a fully functional hot site. If the alternate site was indeed a hot site—as USPTO documentation states—operations would have resumed within minutes or hours of system unavailability in August 2018. Instead, operations were halted for 9 days, hindering USPTO patent examiners from fulfilling their duties and, ultimately, depriving USPTO of its ability to fulfill its mission. This is particularly concerning when factoring in the amount of money that has been expended on the alternate site—more than $28 million and counting—when its primary purpose is to mitigate the effects of disruptive events like the one experienced in August 2018.

While some progress has been made, there is still significant amounts of work to be done to replace or modernize legacy systems. Until then, the Boyers facility will be incapable of providing hot site capabilities. In the meantime, USPTO should revisit the justification for a $4 million annual expenditure and ensure the practicability and efficiency of the Boyers, Pennsylvania, alternative processing site. (See appendix B for further information regarding the potential monetary benefits identified in this report.)

This report presents our findings pertaining to UPSTO's failure to define and establish adequate contingency processes, continued delay to replace decades-old systems, and wasteful use of resources, which ultimately results in the inability to recover from major system disruptions or failures. Currently, USPTO is working to improve its backup and restoration capabilities such as

[16] Legacy software applications were originally developed to run in one location and cannot be replicated to multiple locations. Deploying a legacy system to an alternate location would require modifying and recompiling software code. Developers would need to be familiar with the coding language used by the application and understand exactly how the application functions before making any modifications.

[17] *See* (1) DOC Office of Inspector General, June 13, 2019. *Inadequate Management of Active Directory Puts USPTO's Mission at Significant Cyber Risk*, OIG-19-014-A. Washington, DC: DOC OIG;
(2) DOC OIG, 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; and
(3) DOC OIG, October 16, 2019. *Top Management and Performance Challenges Facing the Department of Commerce*, OIG-20-001. Washington, DC: DOC OIG.

modernizing legacy systems[18] and planning a major contingency plan test that is tentatively scheduled in 2020. However, we are concerned that it took a major system outage and prolonged recovery for USPTO to start developing adequate contingency capabilities, and that we continue to observe delays in the modernization of legacy systems.

Recommendations

We recommend the Under Secretary of Commerce for Intellectual Property and Director of the U.S. Patent and Trademark Office direct the Chief Information Officer to do the following:

1. Implement recommendations outlined in NIST SP 800-34 to ensure that all contingency planning documentation contains the necessary components, including, but not limited to, recovery objectives.
2. Establish a documented process that ensures contingency plan testing includes functional testing that entails simulations of actual system disruption or failure, and that all required participants are involved with contingency plan testing.
3. Ensure that appropriate backup logs are delivered to C3 and backup failures are flagged for review while also establishing a process to alert appropriate personnel who can promptly rectify any failures.
4. Make a determination whether the $4 million in potential monetary benefits that we have identified in this report that is currently allocated for the Boyers alternate site can be used more efficiently.
5. Establish a detailed plan for the replacement of legacy systems and software applications, including milestones and deadlines, and enforce the plan in a manner that holds appropriate personnel accountable.

[18] Current efforts to modernize legacy systems includes the replacement and stabilization of existing legacy software applications.

Summary of Agency Response and OIG Comments

On May 22, 2020, we received USPTO's response to our draft report. In response to our draft report, USPTO concurred with all of our recommendations and described actions it has taken, or will take, to address them. USPTO's complete response, which also included technical comments, is included within this report as appendix C.

In its response, USPTO described actions taken to improve the availability of PALM, including replacing legacy hardware and expanding redundancy of critical data. However, as stated in the response, substantial and continued effort is needed to improve and maintain USPTO business continuity and disaster recovery capabilities.

We are pleased that USPTO concurs with our recommendations and look forward to receiving USPTO's action plan that will provide details on its corrective actions.

Appendix A: Objective, Scope, and Methodology

Our audit objective was to determine whether USPTO has adequate data recovery and contingency plans in place to ensure operational availability of PCAPS. PCAPS is a legacy information system that supports patent application capture, processing, reporting, and retrieval and display.

We judgmentally selected and reviewed the implementation status of internal controls relevant to the audit objective. Specifically, we evaluated fundamental security controls defined in NIST SP 800-53, Revision 4, including contingency planning, contingency plan testing, data backup, data restoration, and implementation of an alternative processing site.

To do so, we performed

- documentation review, including system security plans, most recent security control assessments, contingency plans, and contingency test results;
- interviews of USPTO management, staff, and contractors;
- an inspection of USPTO's alternative processing site at the Iron Mountain facility in Boyers, Pennsylvania; and
- a review of various supporting artifacts, such as backup logs and status reports.

We also 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.
- *U.S. Department of Commerce Information Technology Security Program Policy*, Version 3.2, dated September 2014.
- *United States Patent and Trademark Office IT Security Handbook*, dated March 26, 2018.
- NIST Special Publications:
  - 800-37, Revision 2, *Risk Management Framework for Information Systems: A Security Life Cycle Approach for Security and Privacy*, dated December 20, 2018.
  - 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated January 22, 2015.
  - 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, dated December 18, 2014.
  - 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, dated May 2010.

- 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, dated September 21, 2006.

We did not use computer-generated data as part of this audit.

We conducted our review from March 2019 to October 2019 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. We performed our fieldwork at USPTO headquarters in Alexandria, Virginia, and the Iron Mountain facility in Boyers, Pennsylvania.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B: Potential Monetary Benefits

	Questioned Costs	Unsupported Costs	Potential Funds to Be Put to Better Use
Finding II and **Recommendation 4**			$4,000,000[a]

Source: OIG observations and analysis of USPTO documentation

[a] This amount represents the approximate annual funding of USPTO's alternative processing site that has been underutilized.

Appendix C: Agency Response

UNITED STATES PATENT AND TRADEMARK OFFICE

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

May 22, 2020

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

FROM: Andrei Iancu
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

SUBJECT: Response to Draft Report, Deficiencies in the USPTO's Backup and Restoration Process Could Delay Recovery of Critical Applications in the Event of a System Failure and Adversely Affect Its Mission

Executive Summary

The United States Patent and Trademark Office (USPTO or Agency) appreciates the effort the Inspector General (IG) made in reviewing the Agency's information technology (IT) systems.

As noted in the report, the Patent Capture and Application Processing System (PCAPS) is a critical legacy IT system that allows the USPTO to fulfill its mission of granting patents.

When the Patent Application Locating and Monitoring (PALM) system, which is part of PCAPS, went offline for nine days in August 2018, the mission impact was immediate. However, once the USPTO restored full functionality of the PALM system, aggressive action was taken to reduce the likelihood and mitigate the impact of any such future system failures. Specifically, the USPTO:

- Immediately conducted a post-action analysis to determine the root cause and developed near-term strategies to avoid another outage;
- Secured a third-party vendor to provide an independent, professional assessment and recommendations regarding increasing the stability and ensuring the availability of the PALM system;
- Pursuant to the resulting independent recommendations, replaced legacy server hardware, which resulted in a significant increase in system performance and increased the efficiency, reliability, and overall stability of the PALM system; and

P.O. Box 1450, Alexandria, Virginia 22313-1450 – WWW.USPTO.GOV

- Launched a comprehensive multi-phased initiative, "IT Stabilization, Modernization, and Governance," to review and analyze our existing policies, processes, and practices and to develop implementation plans to improve our business continuity and disaster recovery capabilities. By focusing resources on the highest risk, highest value efforts, we are currently working to replace our legacy IT systems with modern and resilient solutions. That effort is ongoing, with significant executive and staff support.

While these aggressive actions have all been taken since the 2018 outage, the USPTO welcomes and concurs with the recommendations made in the report and will incorporate them into our future action plans. However, given the significant corrective actions that have been initiated by the Agency since the 2018 outage, the USPTO believes that finding I should be appropriately edited to reflect the USPTO's current ability to restore critical applications in the event of a system failure.

Our detailed response to each recommendation follows.

Response to Recommendations

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of the USPTO (1): *Implement recommendations outlined in NIST SP 800-34 to ensure that all contingency planning documentation contains the necessary components, including, but not limited to, recovery objectives.*

USPTO Response:
The USPTO concurs with this recommendation. The Agency will update our most recent contingency plans to align with NIST SP 800-34: Contingency Planning Guide for Federal Information Systems. The USPTO will add missing component information to the contingency plans, including a list of recovery objectives.

Information that is in the System Security Plan or Dynamic Operational Support Plan will be referenced in the Contingency Plan rather than duplicating the same information in order to minimize inaccuracies due to the frequent changes.

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of the USPTO (2): *Establish a documented process that ensures contingency plan testing includes functional testing that entails simulations of actual system disruption or failure and that all required participants are involved with contingency plan testing.*

USPTO Response:
The USPTO concurs with this recommendation. The most recent USPTO PCAPS contingency plan tests will be modified to include:

- A documented process to ensure contingency plan testing includes functional testing;
- Participation from all relevant Office of the Chief Information Officer (OCIO) support teams; and
- Functional testing that involves simulations of actual system disruption or failure.

For the past year, the USPTO has been conducting quarterly controlled shutdown and startup testing of our Lab Data Center to ensure updated procedures are in place, while simulating a failure and recovery situation. The USPTO will also be conducting a planned outage in our Production Data Center that will further exercise these procedures in a controlled manner.

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of the USPTO (3): *Ensure that appropriate backup logs are delivered to C3 and backup failures are flagged for review while also establishing a process to alert appropriate personnel who can promptly rectify any failures.*

USPTO Response:
The USPTO concurs with this recommendation. As part of all standard Production Database Server builds, it is mandatory at the USPTO that backup logs are created. Backups are held locally on the database servers, and the Operating Systems Operations Section backup team copies the information to tape and validates that the backup was completed successfully to ensure adequate storage for subsequent backups.

The USPTO will initiate the following corrective actions:

- Ensure all automated backup jobs are administered nightly; and
- Review and update backup procedures to confirm that coordination and alerting are in place between all OCIO teams involved.

In addition, immediately following the 2018 PALM outage, the USPTO increased the full backup frequency for the PALM Database from once a week to twice a week, with a copy of the redo logs going to more than one location, thereby increasing the Agency's ability to recover these data in the event of a failure.

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of the USPTO (4): *Make a determination whether the $4 million in potential monetary benefits that we have identified in this report and that are currently allocated for the Boyers alternate site can be used more efficiently.*

USPTO Response:
The USPTO concurs with this recommendation. The Agency will make a determination about whether the $4 million in potential monetary benefits that were identified in this report and are currently allocated for the Boyers alternate site can be used more efficiently in the USPTO's comprehensive Business Continuity/Disaster Recovery plans. The USPTO will also conduct market research on the feasibility of relocating and/or standing up new equipment in a facility other than the Boyers alternate site.

While the USPTO agrees with and will conduct a cost-benefit analysis as discussed above, since the 2018 PALM outage, the USPTO has proactively taken action to best utilize the Boyers alternate site. Specifically, the USPTO initiated the following Business Continuity/Disaster

Recovery plan, as a way to increase the USPTO's ability to recover quickly in the event of a critical PALM system database failure:

- Upgraded the PALMPROD Database to the latest supported version, addressing technical debt and increasing database security;
- Built a local Standby PALM Database replica for increased recoverability;
- Built a Boyers Standby PALM Database replica for increased recoverability; and
- Built a Boyers Standby PALM Database replica that will allow the USPTO to redirect application database traffic from the Alexandria campus to the Boyers data center, thereby increasing system availability and recoverability.

To use Boyers Backup Storage as a Service (BSaaS), the USPTO has begun cross-site backups to BSaaS in preparation for the upgrade of the central backup disk storage system to a supported version.

To improve overall alternate processing site infrastructure and disaster recovery readiness, the USPTO is preparing for production deployment of improved network access control, an enhanced network circuit upgrade, independent Enterprise Management System disaster recovery, and standalone capability for security monitoring.

IG Recommendation that the Under Secretary of Commerce for Intellectual Property and Director of the USPTO (5): *Establish a detailed plan for the replacement of legacy systems and software applications, including milestones and deadlines, and enforce the plan in a manner that holds appropriate personnel accountable.*

USPTO Response:
The USPTO concurs with this recommendation. Since the 2018 PALM outage, the USPTO has already taken aggressive action to do this. The OCIO has developed detailed roadmaps for the retirement and next generation deployment of IT systems for every business unit of the USPTO. The OCIO will continue to create and revise detailed roadmaps for legacy system replacement as new information and technology become available. The USPTO will enforce those plans in a manner that holds appropriate personnel accountable.

Conclusion

In closing, the USPTO appreciates the report's findings and recommendations. We remain committed to improving the quality and reliability of our IT systems, and this report, and the recommendations within it, will help us achieve those goals. The OCIO has already made improvements to implement the report's recommendations and is confident in the Agency's ability to satisfy these proposals in timely manner. We look forward to working with the IG as we continue to improve the USPTO's IT security and operations practices.

If additional information is needed regarding USPTO IT systems, please contact:

Don Watson, Chief Information Security Officer and Cybersecurity Division Director, OCIO, USPTO, at 571-272-8130, or by email at .

Liem Nguyen, Cybersecurity Division Information System Security Manager, OCIO, USPTO, at 571-270-0411, or by email at Liem.Nguyen@uspto.gov.

10USPTO00344