Report in Brief

March 24, 2017

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.

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.