U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

United States Patent and Trademark Office

FY 2009 FISMA Assessment of the Patent Cooperation Treaty Search Recordation System (PTOC-018-00)

Final Inspection Report No. OAE-19731
November 2009

Office of Audit and Evaluation

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

NOVEMBER 20, 2009

MEMORANDUM FOR: David Kappos
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

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

SUBJECT: United States Patent and Trademark Office (USPTO)
FY 2009 FISMA Evaluation of Patent Cooperation Treaty Search Recordation System (PTOC-018-00)
Final Report No. OAE-19731

Attached please find a copy of our report on the results of our evaluation of the Patent Cooperation Treaty Search Recordation System (PCTSRS). We evaluated certification and accreditation activities for PCTSRS as part of our responsibilities under the Federal Information Security Management Act (FISMA).

We found only minor deficiencies with the system's certification and accreditation, and continuous monitoring. Likewise, our evaluation of the system's security controls found only minor deficiencies. However, we did not perform a previously scheduled on-site assessment, which would have provided greater assurance of the controls' effectiveness, because it was too close to our FISMA reporting deadline.

Your October 29, 2009, response to our draft report agreed with our findings and recommendations. In our report, we summarize and comment on your response and have included it in its entirety as appendix B.

Please submit to us an action plan within 60 calendar days from the date of this memorandum—this should be in the form of a plan of action and milestones as required by FISMA.

We appreciate the cooperation and courtesies extended to us by your staff during our evaluation. If you would like to discuss any of the issues raised in this report, please call me at (202) 482-1855.

Attachment

cc: Suzanne Hilding, Chief Information Officer, U.S. Department of Commerce
Margaret A. Focarino, acting commissioner for patents, USPTO
John B. Owens II, chief information officer, USPTO
Rod Turk, director, office of policy and governance, USPTO
Welton Lloyd, USPTO audit liaison

Report In Brief

U.S. Department of Commerce, Office of Inspector General

November 2009

United States Patent and Trademark Office (USPTO)

FY 2009 FISMA Assessment of the Patent Cooperation Treaty Search Recordation System (OAE-19731)

Why We Did This Review

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to identify and provide security protection of information collected or maintained by it or on its behalf. Inspectors general are required to annually evaluate agencies' information security programs and practices. Such evaluations must include testing of a representative subset of systems and an assessment, based on that testing, of the entity's compliance with FISMA and applicable requirements.

This review covers our evaluation of USPTO's PCTSRS, which is one of a sample of systems we assessed in FY 2009.

Background

PCTSRS is a contractor-owned system that provides services related to international patent applications. The contractor's employees use the system to perform searches and submit written opinions regarding the patentability of inventions.

C&A is a process by which security controls for IT systems are assessed to determine their overall effectiveness. Understanding the remaining vulnerabilities identified during the assessment is essential in determining the risk to the organization's operations and assets, to individuals, to other organizations, and to the nation resulting from the use of the system.

What We Found

Our objectives for this review were to determine whether (1) implemented controls adequately protect the system and its information, (2) continuous monitoring is keeping the authorizing official sufficiently informed about the operational status and effectiveness of security controls, and (3) the certification and accreditation (C&A) process produced sufficient information about remaining system vulnerabilities to enable the authorizing official to make a credible, risk-based accreditation decision.

Although we found minor deficiencies with PCTSRS' C&A activities, USPTO's C&A process produced sufficient information to enable the authorizing officials to make a credible, risk-based accreditation decision. Our evaluation of the system's security controls also found only minor deficiencies.

What We Recommend

In order to ensure PCTSRS complies with FISMA requirements, USPTO should resolve the minor deficiencies we reported in our assessment. USPTO agrees with our findings, and has begun to take steps to implement our recommendations.

Contents

Introduction

We evaluated certification and accreditation activities for the Patent Cooperation Treaty Search Recordation System (PCTSRS) as part of our FY 2009 responsibilities for conducting independent evaluations under the Federal Information Security Management Act (FISMA). For a complete outline of our objectives, scope, and methodology, see appendix A.

PCTSRS is owned and operated by Cardinal IP, a U.S. Patent and Trademark Office (USPTO) contractor that provides services related to international patent applications. Cardinal employees use the system to perform searches and submit written opinions regarding the patentability of inventions.

An application filed with USPTO under the Patent Cooperation Treaty is transmitted to a PCTSRS batch server via a secure connection. Cardinal staffers then transfer the application to PCTSRS' web docket system and assign an appropriate search professional to work on it. The search professional remotely accesses the "case" from her own computer via a secure remote desktop application, which includes controls to prevent the transfer of patent data to her local disk drive. Cardinal then transfers the search professional's written opinion in its web docket system back to USPTO via a batch server and secure connection.

Based on the intellectual property protection information it contains, PCTSRS is categorized [redacted]

PCTSRS is located at Cardinal IP's [redacted]. The system, which went operational in October 2006, underwent its first security certification in 2008 and was granted an interim authorization to operate in September 2008. Cardinal and USPTO's Information Technology Security Management Group then devised a recertification plan to assess only the controls from the previous assessment that were deemed high risk, that had been changed since the previous assessment, or that were identified by USPTO's independent verification and validation (IV&V) contractor (after the interim authorization to operate was granted) as needing better assessment.

Controls were assessed by a certification team from Veris Group, a contractor for Cardinal IP. The initial scope of 68 controls was later expanded to include all physical and environmental controls pertaining to the [redacted] datacenter, which had not been assessed in 2008. This time, the IV&V contractor reviewed the recertification and accreditation package before the accreditation decision was made. The contractor's review helped improve the security plan and documentation of the control assessment.

In late May 2009, the acting commissioner for patents and the chief information officer—co-authorizing officials—granted an authorization to operate. In the accreditation decision letter, the officials noted that vulnerabilities in Configuration

Settings (CM-6) and Flaw Remediation (SI-2)[1] were "a concern" and directed Cardinal "to immediately begin the remediation efforts for these vulnerabilities and complete implementation as soon as possible, but no later than 90 days after the date of this [authorization to operate]. Additionally, the contractor shall provide bi-weekly status reports toward remediation of these vulnerabilities."[2]

[1] "CM-6," "SI-2" and other similarly formatted notations are security control identifiers from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems.* We include the name of the control at the first mention in the report and use the identifier thereafter.
[2] Owens, John B. II, and Margaret A. Focarino. May 7, 2009. *Security Certification Statement for the Patent Cooperation Treaty Search Recordation System.* Memorandum to Blaine Copenheaver, USPTO, and Rod Turk, USPTO.

Findings and Recommendations

I. Certification and Accreditation Process Included Minor Deficiencies

Although we found deficiencies with PCTSRS' certification and accreditation activities, USPTO's process for certifying contractor systems produced sufficient information to enable the co-authorizing officials to make a credible, risk-based accreditation decision.

A. Boundary Definition and System Component Inventory

The system accreditation boundary definition was not updated for two key classes of components: [redacted] The system boundary document described four [redacted] components [redacted]) in PCTSRS. Also, a spreadsheet presented as the system's component inventory and referred to in the initiation-phase security plan did not mention any [redacted] components. However, we learned there are actually 12 [redacted] components considered to transmit PCTSRS data: in addition to the 4 mentioned in the system boundary definition, there are 8 other [redacted]. This deficiency did not detract from the control assessment, as all 12 were assessed for compliance with secure configuration settings.

[redacted] and a [redacted] were included in the information system component inventory presented in the certification and accreditation package and in a second list used by the certification team to validate the Information System Component Inventory (CM-8) security control. These components were scanned for vulnerabilities, but no additional assessments were conducted by the certification team. Cardinal staff told us these components do not process, store, or transmit PCTSRS data; therefore, the components are considered to be out of scope. We did not perform an on-site assessment to validate that this was the case. Cardinal staff told us they intend to revise CM-8 documentation to reflect the fact that these [redacted] are not within the scope of the system's boundary.

B. Security Plan Deficiencies

The post-certification security plan[3] indicates that the "details of the [information system component] inventory are documented in this [system security plan]," and that Cardinal "updates the PCTSRS inventory as an integral part of system management."[4] However, the CM-8 issues discussed above suggest otherwise, and Cardinal staff conceded that the evidence they provided to the certification team for CM-8 was outdated. The security plan and related procedures for CM-8 did not provide any details as to how the component inventory was maintained or what information it contained, nor a reference to the actual inventory itself. The

[3] We reviewed version 2.6 of the system security plan, which was the basis for the accreditation decision. Late in our evaluation, we were given version 3.0 (dated July 16, 2009) of the security plan and found the same deficiencies.
[4] U.S. Patent and Trademark Office, April 16, 2009. *Cardinal Intellectual Property (CIP) Patent Cooperation Treaty Search Recordation System (PCTSRS) System Security Plan (SSP), Version 2.6*, 69-70.

descriptions amounted to mere assertions that the control requirements were being met.

We noted a discrepancy between the parameters for Unsuccessful Login Attempts (AC-7) described in the security plan and the [redacted] for PCTSRS that was included in the control assessment artifacts. The security plan stated that [redacted]. AC-7 was not assessed for the 2009 recertification, so this discrepancy was not addressed by the certification team. However, Cardinal staff confirmed our conclusion that the change was the result of implementing secure configuration settings in [redacted] environments.

Account Management (AC-2), enhancement 4, requires the organization to employ automated mechanisms to audit account creation, modification, disabling, and termination. However, the PCTSRS security plan descriptions of mechanisms for the various component types do not address auditing capabilities.

II. Minor Deficiencies Identified in System Security Controls

We identified only minor control deficiencies in our review of system artifacts and interviews of contractor staff.

A. Configuration Settings (CM-6)

Secure configuration settings were not defined prior to the control assessment, but the eventual benchmarks were identified and settings examined on [redacted]. The certification team concluded CM-6 was "other than satisfied," discussed the vulnerability in the security assessment report, and added CM-6 to the system's plan of action and milestones (POA&M). Cardinal has now defined secure configuration settings for [redacted].

Secure configuration settings defined for [redacted] components are included in PCTSRS' [redacted] *Standards*. Unlike the other configuration settings defined for IT products mentioned above, this document does not compare PCTSRS' defined settings to industry benchmark settings. While there is overlap with the industry benchmark, not all recommended settings were addressed—a particular concern involves [redacted].

Cardinal has recently submitted evidence to USPTO's IT security management group in support of closing the POA&M for CM-6. USPTO's IV&V contractor is currently evaluating the evidence for completeness. However, we found no evidence that [redacted] devices were compliant with PCTSRS' defined settings. The certification

team noted in its assessment of CM-6 that "benchmark tests conducted against [redacted] [emphasis added] confirmed that system configuration settings are not compliant with the [industry] benchmark standard."

B. Baseline Configuration (CM-2)

The requirements for this control were at least partially confused with the requirements for Configuration Settings (CM-6) in the initiation, security certification, and accreditation phases. As a result, the control requirements are not being properly remediated in the (current) continuous monitoring phase.

The security plan, the control assessment, and the security assessment report all indicated that, with respect to CM-2 requirements, Cardinal IP administrators were in the process of implementing secure configuration settings (i.e., CM-6) based on industry benchmarks. The *Cardinal Intellectual Property Security Control Procedures* for CM-2 further discussed CM-6 requirements rather than what was needed for the system's baseline configuration. Although the control was deemed "other than satisfied," the certification team's evidence for this status was a USPTO memo addressing secure configuration settings, which again falls under CM-6 requirements.

Currently, Cardinal has submitted a request to close the CM-2-related POA&M item along with the CM-6 POA&M item. However, only compliance scans validating secure configuration settings were submitted as proof of the control's remediation.

As explained in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*,

> [CM-2] establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture.[5]

We reviewed two reports prepared by Cardinal that detail the applications installed in workstations. The information in the reports would partially satisfy CM-2 requirements for those components.

[5] NIST Special Publication 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, F-24.

III. Continuous Monitoring Is Keeping Authorizing Officials Sufficiently Informed, with a Minor Exception

Continuous monitoring—with respect to configuration management and the USPTO POA&M process—does appear to be keeping the authorizing officials sufficiently informed about the operational status and effectiveness of security controls, although minor deficiencies should be remediated.

Cardinal has made considerable progress made towards implementing CM-6 and SI-2, and has provided bi-weekly status updates to USPTO in accordance with the authorizing officials' directive. However, we did note a deficiency in the remediation of SI-2 vulnerabilities.

A. Vulnerability Remediation and POA&M Validation

USPTO closed the SI-2 weakness in the system's POA&M without properly validating that vulnerabilities had been fully remediated. We reviewed the notes and artifacts supporting the closing of a POA&M item that stemmed from the certification team's assessment of SI-2. Both the explanation for closing the POA&M item and the artifacts included as evidence of the vulnerabilities' remediation referred to workstations only, not to servers.

However, the vulnerabilities identified by the certification team pertained to both workstations and servers (from the certification team's assessment): "Although the [redacted] server and [redacted] workstation environments are patched, outdated and insecure versions of third party software were detected *throughout the environment* [emphasis added]. Most notably, vulnerabilities were associated with outdated installations of [redacted]." The evidence for SI-2 assessment pointed to findings from vulnerability scans. A sorting of scan results indicates 297 high- or medium-risk findings (184 high) related to SI-2 for [redacted] servers.

After we discussed this deficiency with USPTO and Cardinal staff, they produced archived emails with attached evidence that Cardinal had fixed the server vulnerabilities. However, USPTO did not follow its own procedures and include the evidence in the POA&M record; based on the notes supporting the closing of the SI-2 POA&M item, USPTO's validation pertained to workstations only.

Recommendations

USPTO should

1. review the information system component inventory and update it in accordance with the requirements of USPTO policy and NIST SP 800-53;
2. correct the security plan deficiencies (including related security control procedures) with accurate and complete information;
3. revise the PCTSRS mandatory configuration settings for [redacted] components to address the deficiencies described above;
4. revise the security plan description for CM-2 and remediate the POA&M item in accordance with the actual control requirements; and
5. reopen the SI-2 POA&M item until evidence of remediation of outdated software on server components is validated in accordance with USPTO procedure.

Summary of USPTO Response and OIG Comments

In response to our draft report, USPTO agreed with our findings and recommendations. USPTO also described actions it intends to take to remediate the deficiencies—these were consistent with our recommendations. USPTO's response is included in this report as appendix B.

Appendix A: Objectives, Scope, and Methodology

Our objectives were to determine whether (1) implemented controls adequately protect the system and its information, (2) continuous monitoring is keeping the authorizing official sufficiently informed about the operational status and effectiveness of security controls, and (3) the certification and accreditation process produced sufficient information about remaining system vulnerabilities to enable the authorizing official to make a credible, risk-based accreditation decision.

Security certification and accreditation packages contain three elements, which form the basis of an authorizing official's decision to accredit a system:

- The **system security plan** describes the system, the requirements for security controls, and the details of how the requirements are being met. The security plan provides a basis for assessing security controls and also includes other documents such as the system risk assessment and contingency plan, per Department policy.

- The **security assessment report** presents the results of the security assessment and recommendations for correcting control deficiencies or mitigating identified vulnerabilities. This report is prepared by the certification agent.

- The **plan of action & milestones (POA&M)** is based on the results of the security assessment. It documents actions taken or planned to address remaining vulnerabilities in the system.

The Department's *IT Security Program Policy and Minimum Implementation Standards* requires that certification and accreditation packages contain a certification documentation package of supporting evidence of the adequacy of the security assessment. Two important components of this documentation are

- the **certification test plan**, which documents the scope and procedures for testing (assessing) the system's ability to meet control requirements; and

- the **certification test results**, which is the raw data collected during the assessment.

To evaluate the certification and accreditation, we reviewed all components of the certification and accreditation package and interviewed USPTO and Cardinal staff to clarify any apparent omissions or discrepancies in the documentation and gain further insight on the extent of the security assessment. We evaluated the security

plan and assessment results for applicable security controls and will give substantial weight to the evidence that supports the rigor of the security assessment when reporting our findings to OMB.

To evaluate system security controls, we examined system artifacts included in the package as well as additional information and evidence about controls we requested during the course of our review. We also interviewed Cardinal and USPTO staff to gain further insight on the status of controls. Our FISMA reporting deadline caused us to cancel previously scheduled on-site assessments of PCTSRS controls, which we would typically do and which we would weigh significantly when determining the effectiveness of system security controls.

To evaluate continuous monitoring, we conducted interviews and examined correspondence and other information exchanged between Cardinal and USPTO since the accreditation and the system's POA&M records.

We used the following review criteria:

- Federal Information Security Management Act of 2002 (FISMA)
- U.S. Department of Commerce *IT Security Program Policy and Minimum Implementation Standards*, June 30, 2005
- NIST Federal Information Processing Standards (FIPS)
    - Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
    - Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publications:
    - 800-18, *Guide for Developing Security Plans for Information Technology Systems*
    - 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
    - 800-53, *Recommended Security Controls for Federal Information Systems*
    - 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
    - 800-70, *Security Configuration Checklists Program for IT Products*

- 800-115, *Technical Guide to Information Security Testing and Assessment*

We conducted our evaluation in accordance with the Inspector General Act of 1978, as amended, and the *Quality Standards for Inspections* (revised January 2005), issued by the President's Council on Integrity and Efficiency.

Appendix B: USPTO Response

UNITED STATES PATENT AND TRADEMARK OFFICE

Office of the Chief Information Officer

October 29, 2009

MEMORANDUM FOR: Allen Crawley
Assistant Inspector General for System Acquisition and IT Security, Office of Inspector General
Department of Commerce

THROUGH: Barry K. Hudson
Chief Financial Officer
United States Patent and Trademark Office

FROM: John B. Owens II
Chief Information Officer
United States Patent and Trademark Office

SUBJECT: Response to FY 2009 FISMA Assessment of the Patent Cooperation Treaty Search Recordation System (PTOC-018-00)
Draft Inspection Report No. OAE-19731, September 2009

Thank you for your draft report to the Honorable Under Secretary and Director David Kappos dated September 29, 2009, detailing your findings and recommendations. We appreciate the effort your staff has made in evaluating the effectiveness of our Patent Cooperation treaty Search Recordation Information System. We have carefully considered the recommendations made in the subject draft report and concur with your recommendations. The United States Patent and Trademark Office (USPTO) provides the following attachment as our response to these recommendations.

Again, we thank the Assistant Inspector General for System Acquisition and IT Security for the report. We intend to meet the recommendations in a diligent manner, and we will gratefully accept suggestions as we move forward to ensure that an effective security program is in place that will enable us to attain the needs of the USPTO.

Attachment

USPTO Cyber Security Division's Response to FY 2009 FISMA Assessment of the Patent Cooperation Treaty Search Recordation System (PTOC-018-00) Draft Inspection Report No. OAE-19731, September 2009

OIG Finding:
System accreditation boundary definition was not updated for two key classes of components:
[redacted]

USPTO Response:

USPTO agrees with this finding. The System Accreditation Boundary document and the System Security Plan will be reviewed and updated to include the missing items identified by the OIG Inspection. Both documents will be modified so that they contain an up-to-date inventory of all devices that store, transmit, or process USPTO data.

OIG Finding:
Security Plan Deficiencies:

- *Information System Component Inventory (CM-8) –the security plan and related procedures did not provide any details as to how the component inventory was maintained or what information it contain, nor a reference to the actual inventory itself.*

[redacted]

- *Account Management (AC-2) enhancement 4 –the PCTSRS security plan descriptions of mechanisms for the various component types do not address auditing capabilities.*

USPTO Response:

USPTO agrees with these findings and will update the security plan in the following ways:

- In response to the CM-8 deficiency, Cardinal will document a full detailed inventory of all devices that store, transmit, or process USPTO data along with relevant ownership of all active devices. This inventory will include information determined to be necessary to achieve effective property accountability.
- In response to the AC-7 deficiency, Cardinal will update the System Security Plan document to reflect the change in the number of unsuccessful logins that will result in account lockout.

[redacted]

- In response to the AC-2 enhancement 4 deficiency, Cardinal will update the SSP document to

[redacted]

OIG Finding:
The PCTSRS document [redacted] *Standards* does not compare PCTSRS' defined settings for [redacted] devices to industry benchmark settings. Not all recommended settings were addressed – a particular concern involves [redacted].

USPTO Response:

USPTO agrees with this finding. Cardinal will write new secure baseline documentation to outline the mandatory configuration settings for [redacted] components. This new secure baseline documentation will be based on the CIS industry standard security benchmark for [redacted] and will define any required deviation from the CIS benchmark. Cardinal will also scan all [redacted] components to verify compliance.

OIG Finding:
The requirements for the control Baseline Configuration (CM-2) were at least partially confused with the requirements for Configuration Settings (CM-6) in the initiation, security certification, and accreditation phases. As a result, the control requirements are not being properly remediated in the (current) continuous monitoring phase.

USPTO Response:

USPTO agrees with this finding. Cardinal will create a report that details the makeup of each component of the PCTSRS information system. This report will include all installed software, updated patch information, and the logical placement for each component in the PCTSRS information system architecture.

OIG Finding:
The SI-2 vulnerability was closed in the system's POA&M without supporting evidence that it had been fully remediated.

USPTO Response:

USPTO agrees with this finding. USPTO will reopen the SI-2 POA&M and upload evidence into CSAM showing that Cardinal had fixed the server vulnerabilities.