U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

United States Patent and Trademark Office

FY 2009 FISMA Assessment of Enterprise UNIX Services System (EUS) (PTOI-010-00)

Final Inspection Report No. OAE-19729
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

Allen Crawley

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

SUBJECT: United States Patent and Trademark Office
FY 2009 FISMA Assessment of Enterprise UNIX Services System (EUS) (PTOI-010-00)
Final Inspection Report No. OAE-19729

This report presents the results of our Federal Information Security Management Act (FISMA) review of USPTO's certification and accreditation of the Enterprise UNIX Services system.

We found that the authorizing official received sufficient information to make a credible, risk-based decision to approve system operation. However, we also identified several security plan inaccuracies and control assessment deficiencies, and OIG's own assessment of selected security controls found vulnerabilities that require remediation.

In its response to our draft report, USPTO concurred with all our findings and recommendations. USPTO's response is summarized in the appropriate sections of the report. USPTO's response is included in its entirety as appendix A.

We request that you provide us with an action plan describing the actions you have taken or plan to take in response to our recommendations within 60 calendar days of the date of this report. A plan of action and milestones should be used to communicate the plan 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
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

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 EUS system, which is one of a sample of systems we assessed in FY 2009.

Background

EUS is a general support system that comprises various operating systems and databases. The purpose of this system is to provide a hosting platform and databases that support major USPTO applications.

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.

United States Patent and Trademark Office (USPTO)

FY 2009 FISMA Assessment of the Enterprise UNIX Services System (OAE-19729)

What We Found

We evaluated certification and accreditation activities for the Enterprise UNIX Services (EUS) system as part of our FY 2009 reporting responsibilities under the Federal Information Security Management Act (FISMA).

We found that while the security plan was generally adequate, some inaccuracies need to be addressed. Security control assessments were generally adequate but improvements are needed, and our control assessment found some vulnerabilities that require remediation. Despite these deficiencies, the authorizing official received sufficient information to make a credible, risk-based decision to approve system operation.

What We Recommend

In order to ensure the EUS system complies with FISMA requirements, USPTO should resolve the deficiencies we reported. USPTO agrees with our findings, and has identified the corrective actions it needs to take to address our recommendations.

Listing of Abbreviated Terms and Acronyms

AIS	automated information system
C&A	certification and accreditation
CALS	Centralized Audit Log System
ERA	Enterprise Remote Access
EUS	Enterprise UNIX Services
FISMA	Federal Information Security Management Act of 2002
IT	information technology
[redacted]	[redacted]
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NSI	Network and Security Infrastructure
[redacted]	[redacted]
SSP	system security plan
USPTO	United States Patent and Trademark Office
USSS	UNIX Systems Services Section

Synopsis of Findings

- Security plan was generally adequate but inaccuracies need to be addressed.
- Security control assessments were generally adequate but improvements are needed.
- OIG control assessment found vulnerabilities requiring remediation.

Conclusion

Despite security plan inaccuracies and control assessment deficiencies, the authorizing official received sufficient information to make a credible, risk-based decision to approve system operation.

Summary of USPTO Response

In its response to our draft report, the United States Patent and Trademark Office (USPTO) concurred with all of our findings and recommendations (see appendix A). USPTO requested additional information related to one of our findings.

In addition, USPTO identified actions it will take to address our findings and recommendations.

OIG Comments

USPTO concurred with our findings and recommendations and provided corrective actions to address them.

We also provided the requested information to USPTO. We address specific elements of USPTO's response in the applicable sections of the report.

Introduction

We evaluated the certification and accreditation for the Enterprise UNIX Services (EUS) system. For our complete objectives, scope, and methodology, see appendix B.

The EUS system is a general support system that comprises UNIX-based operating systems and [redacted] databases. The purpose of this system is to provide a hosting platform and databases that support major USPTO applications. The system was authorized to operate on May 5, 2009. At that time, there were [redacted].

USPTO has characterized EUS as a [redacted] effect on organizational operations, organizational assets, or individuals.

Findings and Recommendations

1. Security Plan was Generally Adequate but Inaccuracies Need to be Addressed

- The initiation-phase security plan generally provided adequate implementation descriptions for applicable security controls and identified controls as system-specific, common,[1] or hybrid.[2]
  - The security plan referenced system boundary documents that adequately described the accreditation boundary.

- The security plan was updated to reflect the results of security certification; however, some improvements are needed.
  - The initiation phase security plan identified 54 controls with system-specific implementations. However, during the certification phase, 11 additional system-specific controls were identified.
  - The security plan states that the control Session Authenticity (SC-23) is not applicable to the system. [redacted] Thus, the control is applicable to EUS and should be described in the security plan.
  - The security plan states that the control Time Stamps (AU-8) is a common control. However, information technology (IT) products in the system must be configured to use the appropriate time server. This configuration setting is the responsibility of EUS, so AU-8 should be identified as a hybrid control.
  - The following security control implementation descriptions need improvement.
    - Access Enforcement (AC-3). [redacted]
    - Response to Audit Processing Failures (AU-5). The control description only addresses file system capacity and does not address other failures such as failure in the [redacted].
    - User Identification and Authentication (IA-2). The control description does not reference appropriate policies that identify USPTO requirements for password complexity. As a result, these requirements were not assessed (see finding 3).
    - Configuration Settings (CM-6). [redacted]

[1] Common control: a security control that applies to one or more agency systems. A common control is developed, implemented, and assessed by a responsible official other than the information system owner.

[2] Hybrid control: a designation given to a security control in situations in which one part of the control is deemed to be common, while another part of the control is deemed to be system-specific.

[3] [redacted]

Recommendation

1.1 USPTO should ensure that the security plan is updated to correct the inaccuracies noted.

USPTO Response

USPTO concurred with this finding and our recommendation.

2. Security Control Assessments Were Generally Adequate but Improvements Are Needed

- System-specific control assessments were generally adequate.
  - Assessments were performed on an adequate set of system components.
  - Results, in general, were sufficiently supported by evidence.
  - Procedures were adequate to assess security control requirements.

- Controls implemented on [redacted] servers were not adequately assessed.
  - The servers were scanned for vulnerabilities.
  - Certification test results indicate that two controls were assessed. However, issues identified during the assessment were not reported to the authorizing official, recorded in the security assessment report, or included in the plan of action and milestones.
    - [redacted]
    - [redacted]
  - Eighteen additional controls implemented on these servers were not assessed (for example, controls from the [redacted] families).

- Assessments of the following controls on the UNIX-based servers were inadequate.
  - Control assessments for Access Enforcement (AC-3) [redacted]
  - Control assessments for User Identification and Authentication (IA-2) [redacted]
  - Compliance scans to assess Authenticator Management (IA-5) [redacted]

- Assessment results were not included for the following security controls that are provided by other systems.
  - [redacted] The security plan states that the system relies on the CALS, which is part of the Network and Security Infrastructure system.
  - [redacted] The security plan states that this control is provided by another system but does not identify the system.
  - [redacted] The security plan states that this control is provided by the Enterprise Remote Access (ERA) system.
  - [redacted] The security plan states that this is provided by CALS.
  - [redacted] The security plan states that this control is provided by ERA.

- Assessment procedures for the following common security controls called for an examination or test of actual system components, but only document reviews or interviews were conducted.
  - [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Recommendations

USPTO should ensure that

2.1 controls implemented on the [redacted] are assessed and any deficiencies are briefed to the authorizing official and appropriate plan of action and milestones items are created;
2.2 inadequacies identified for security controls AC-3, IA-2, and IA-5 are corrected prior to conducting future control assessments;
2.3 assessment results for controls provided by other systems are presented to the authorizing official; and
2.4 common control assessment procedures requiring an examination or test of system components are performed.

USPTO Response

USPTO concurred with this finding and our recommendations. USPTO requested that we identify the 18 additional controls that were not assessed on [redacted] so it could plan appropriate corrective actions.

OIG Comments

We provided USPTO the requested information via e-mail.

3. OIG Control Assessment Found Vulnerabilities Requiring Remediation

As part of OIG's FY 2009 Federal Information Security Management Act of 2002 (FISMA) evaluation of EUS, we assessed a targeted set of system components to determine if selected security controls are properly assessed and implemented on applicable IT products. We tailored our procedures to the system's specific control implementations.

- OIG assessments identified the following weaknesses in National Institute of Standards and Technology Special Publication (NIST SP) 800-53 controls that were not identified by the certification team and need to be addressed.
  - [redacted]
    - [redacted]
  - [redacted]
    - [redacted]
- Details of NIST SP 800-53 controls that we assessed are listed in table 1.
- Components selected for OIG control assessment are listed in appendix C.

Recommendation

3.1 USPTO should add the vulnerabilities identified in table 1 to the system's plan of action and milestones and remediate them accordingly.

USPTO Response

USPTO concurred with this finding and our recommendation.

[5] [redacted]

Table 1. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	EUS Assessment Results (Excerpts)	OIG Assessment Results
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Table 1. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	EUS Assessment Results (Excerpts)	OIG Assessment Results
[redacted]	[redacted]	[redacted]	[redacted]

Table 1. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	EUS Assessment Results (Excerpts)	OIG Assessment Results
[redacted]	[redacted]	[redacted]	[redacted]

Table 1. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	EUS Assessment Results (Excerpts)	OIG Assessment Results
[redacted]	[redacted]	[redacted]	[redacted]
		[redacted]	[redacted]
		[redacted]	

Table 1. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	EUS Assessment Results (Excerpts)	OIG Assessment Results
[redacted]	[redacted]	[redacted]	[redacted]

Table 1. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	EUS Assessment Results (Excerpts)	OIG Assessment Results
[redacted]	[redacted]	[redacted]	[redacted]

Table 1. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	EUS Assessment Results (Excerpts)	OIG Assessment Results
[redacted]	[redacted]	[redacted]	[redacted]

Appendix A: USPTO's Response to Findings

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 Enterprise UNIX Services System (EUS) (PTOI-010-00), Draft Inspection Report No. OAE-19729/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 EUS 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's Response to FY 2009 FISMA Assessment of Enterprise UNIX Services System (EUS) (PTOI-010-00), Draft Inspection Report No. OAE-19729/September 2009

OIG Finding:

1. *Security Plan was Generally Adequate but Inaccuracies Need to be Addressed.*

- *The security plan was updated to reflect the results of security certification; however, some improvements are needed.*
  - *The initiation phase security plan identified 54 controls with system-specific implementations. However, during the certification phase, 11 additional system-specific controls were identified.*
  - *The security plan states that the control Session Authenticity (SC-23) is not applicable to the system.* [redacted] *Thus, the control is applicable to EUS and should be described in the security plan.*
  - *The security plan states that the control Time Stamps (AU-8) is a common control. However, IT products in the system must be configured to use the appropriate time server. This configuration setting is the responsibility of EUS, so AU-8 should be identified as a hybrid control.*
  - *The following security control implementation descriptions need improvement.*
    - *Access Enforcement (AC-3).* [redacted]
    - *Response to Audit Processing Failures (AU-5). The control description only addresses file system capacity and does not address other failures such as failure in the* [redacted]
    - *User Identification and Authentication (IA-2). The control description does not reference appropriate policies that identify USPTO requirements for password complexity. As a result, password complexity requirements were not assessed (see finding 3).*
    - *Configuration Settings (CM-6).* [redacted]

USPTO Response:

USPTO agrees with this finding. The security plan will be reviewed and updated to include the missing items identified by the OIG inspection.

- The system-specific controls will be added to the security plan.

Page 1 of 5

- The implementation description for SC-23 will be updated to reflect the applicability to the system.
- The implementation description for AU-8 will be updated to reflect the status as a hybrid control.
- The implementation description for AC-3 will be updated [redacted].
- The implementation description for AU-5 will be updated to address other failures of the audit processing system.
- The implementation description for IA-2 will be updated to reference and state the requirements for password complexity.
- The implementation description for will be updated to reflect the responsibility of EUS for [redacted] security settings.

OIG Finding:

2. *Security Control Assessments Were Generally Adequate but Improvements Are Needed*

- *Controls implemented on* [redacted] *servers were not adequately assessed.*
  - [redacted]
  - [redacted]
  - *Eighteen additional controls implemented on these servers were not assessed.*

- *Assessments of the following controls on the UNIX-based servers were inadequate.*
  - *Control assessments for Access Enforcement (AC-3)* [redacted]
  - *Control assessments for User Identification and Authentication (IA-2)* [redacted]
  - *Compliance scans to assess Authenticator Management (IA-5)* [redacted]

- *Assessment results were not included for the following security controls that are provided by other systems.*
  - [redacted] *The security plan states that the system relies on the Centralized Audit Log System (CALS), which is part of the Network and Security Infrastructure (NSI) system.*
  - [redacted] *The security plan states that this control is provided by another system but does not identify the system.*
  - [redacted] *The security plan states that this control is provided by the Enterprise Remote Access (ERA) system.*
  - [redacted] *The security plan states that this control is provided by CALS and that "Anomalous behavior is monitored by the Network Security Operations Center (NSOC)."*
  - [redacted] *The security plan states that this is provided by CALS.*

Page 2 of 5

- [redacted] *The security plan states that this control is provided by ERA.*

- *Assessment procedures for the following common security controls called for an examination or test of actual system components, but only document reviews or interviews were conducted.*
  - [redacted]

USPTO Response:

USPTO agrees with this finding and will address each control as required. For the [redacted] Servers, USPTO will take the following actions:

- [redacted]

USPTO recommends that OIG identify the 18 additional NIST 800-53 controls that were identified as not assessed so that corrective action is taken in Fiscal Year 2010.

For controls assess on the UNIX-based servers deemed inadequate, USPTO will take the following actions:

- For the AC -3, IA-2, and IA-5 controls, an OPG-CSD independent security assessor will reassess the security control.

For the security controls that are provided by other systems, USPTO will take the following actions:

- For the [redacted] control, an OPG-CSD independent security assessor will obtain the assessment results from NSI and present them to the authorizing official.

- For the [redacted] control, an OPG-CSD independent security assessor will identify the system this control is inherited from. The assessment results will be obtained and presented to the authorizing official.
- For the [redacted] control, an OPG-CSD independent security assessor will obtain the assessment results from ERA and present them to the authorizing official.
- For the [redacted] control, an OPG-CSD independent security assessor will obtain the assessment results from NSI and present them to the authorizing official.
- For the [redacted] and [redacted] controls, an OPG-CSD independent security assessor will obtain the assessment results from NSI and present them to the authorizing official.
- For the [redacted] control, an OPG-CSD independent security assessor will obtain the assessment results from ERA and present them to the authorizing official.

For the security controls that were inadequately examined or tested, USPTO will take the following actions:

- For the [redacted] controls, an OPG-CSD independent security assessor will reassess the security controls using appropriate procedures.

OIG Finding:

3. *OIG Control Assessment Found Vulnerabilities Requiring Remediation*

As part of OIG's FY 2009 FISMA evaluation of EUS, we assessed a targeted set of system components to determine if selected security controls are properly assessed and implemented on applicable IT products. We tailored our procedures to the system's specific control implementations.

- *OIG assessments identified the following weaknesses in NIST SP 800-53 controls that were not identified by the certification team and need to be addressed.*
  - [redacted]
    - [redacted]
  - [redacted]
    - [redacted]

USPTO Response:

USPTO agrees with this finding. In response to the [redacted] section, USPTO has an active project to deploy [redacted] to address the [redacted] POA&M and use [redacted]

[redacted]. In response to the [redacted] Section, USPTO will deploy an updated standardized [redacted].

Regarding each section in table 1, USPTO will take the following actions:

- [redacted]

Page 5 of 5

Appendix B: Objectives, Scope, and Methodology

To meet FY 2009 FISMA reporting requirements, we evaluated the certification and accreditation for the United States Patent and Trademark Office (USPTO) Enterprise UNIX Services (EUS) system.

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 and milestones** 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 (C&A) 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 C&A package and interviewed USPTO 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 the Office of Management and Budget.

In addition, we performed our own assessment of a targeted selection of controls (see appendix B-1). We conducted our assessment using a subset of procedures from NIST SP 800-53A, which we tailored to EUS' specific control implementations. We did not attempt to perform a complete assessment of each control; instead we chose to focus on specific technical and operational elements.

We assessed controls on key classes of IT components, choosing a targeted set of components from each class that would allow for direct comparison with USPTO's certification test results. We assessed controls on [redacted] and [redacted]. We also performed compliance scanning using Nessus.

Our assessment included the following activities:

- extraction, examination, and verification of system configurations
- execution of scripts and manual checklists
- examination of system logs
- review of account management procedures
- vulnerability scanning of network-addressable components

- examination/analysis of security plan descriptions, including related policy and procedure documents
- interviews with appropriate USPTO personnel

Our assessment was limited in scope and should not be interpreted as the comprehensive review that a security certification for a [redacted] system would require. It gave us direct assurance of the status of select aspects of important system controls and provided meaningful comparison with USPTO's security certification.

We used the following review criteria:

- FISMA
- U.S. Department of Commerce *IT Security Program Policy and Minimum Implementation Standards*, June 30, 2005
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards
    - 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-1: NIST SP 800-53 Security Controls Assessed by OIG

- AC-2 Account Management, Enhancements 1 to 4
- AC-3 Access Enforcement
- AC-6 Least Privilege
- AC-7 Unsuccessful Login Attempts
- AC-8 System Use Notification
- AU-6 Audit Monitoring, Analysis, and Reporting
- AU-8 Time Stamps
- IA-2 User Identification and Authentication
- IA-5 Authenticator Management

Appendix C: Components Assessed by OIG

Name	IP Address	Zone	Operating System
[redacted]	[redacted]	[redacted]	[redacted]