U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

United States Patent and Trademark Office

Stronger Management Controls Needed For the Patent Application Capture and Review Automated Information System

Final Report No. OSE-14926/August 2002

PUBLIC RELEASE

Office of Systems Evaluation

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

AUG 22 2002

MEMORANDUM FOR: Nicholas P. Godici
Commissioner for Patents
United States Patent and Trademark Office

Douglas J. Bourgeois
Chief Information Officer
United States Patent and Trademark Office

FROM: Johnnie E. Frazier

SUBJECT: *Stronger Management Controls Needed for the Patent Application Capture and Review Automated Information System*
Final Inspection Report No. OSE-14926

This is the final report on our assessment of information security controls for the United States Patent and Trademark Office's (USPTO's) Patent Application Capture and Review (PACR) Automated Information System. PACR captures, stores, and maintains digital images of U.S. patent applications, and retrieves and prints these documents as needed. USPTO relies on the highly sensitive PACR system for day-to-day operations.

Our evaluation concluded that physical security measures in place during our assessment generally provide appropriate protection for PACR equipment. We further determined, however, that a risk assessment has not been conducted, the security plan is not approved, security controls have not been tested and reviewed, contingency planning is needed, and specialized security training is needed.

Under the Government Information Security Reform Act, information security is the responsibility of federal agency senior management—the agency head, senior managers, and the chief information officer (CIO). The agency head has overall responsibility for ensuring the security of information and information systems supporting agency operations and assets, and senior officials are responsible for the information security of the systems that support their mission. Thus, the Commissioner for Patents is responsible for PACR information security. The agency CIO is required to administer the information security program agency wide, including assisting senior agency officials concerning their responsibilities.

In your written response to our draft report, you agreed with all our recommendations and described corrective actions being taken or planned. The complete response is included as an attachment to this report and constitutes the action plan. We appreciate the cooperation and courtesies extended to us by USPTO in conducting our review.

Attachment

cc: James Rogan, Under Secretary of Commerce For Intellectual Property and Director of the United States Patent and Trademark Office

INTRODUCTION

The Government Information Security Reform Act (GISRA) requires all federal agencies to perform annual reviews of their information security programs and requires the Office of Inspector General (OIG) for each agency to conduct independent evaluations of those programs. As part of our effort to fulfill this requirement, in March 2002 we issued a report, *Additional Senior Management Attention Needed To Strengthen USPTO's Information Security Program*[1], which evaluated the United States Patent and Trademark Office's (USPTO's) information security policies and procedures, roles and responsibilities, and adherence to applicable laws, regulations, and guidance.

GISRA requires each agency's OIG to also conduct reviews of security controls for individual systems. To help fulfill this requirement and as a follow-on effort to our earlier USPTO entitywide review, we chose to evaluate security controls for USPTO's Patent Application Capture and Review (PACR) system because PACR is a highly sensitive system necessary to USPTO's daily operations.

BACKGROUND

PACR provides the capture, storage, maintenance, retrieval, and printing of digital images of U.S. patent applications. PACR relies on USPTO's local area network (LAN), PTONet, to support data processing associated with patent applications. At the time we selected PACR for review, version 3.0 was the operational system. At our entrance conference with USPTO on January 29, 2002, USPTO informed us that the Cylink Secure Domain Units used to encrypt patent application data transmitted on PTONet had been replaced by Redbrook Ravlin encryption devices. The transition from the Cylink to the Ravlin devices had been planned as part of the upgrade to PACR version 3.5, scheduled for deployment in March 2002. The deployment occurred in March as anticipated, and PACR version 3.5 included the transition to the Ravlin devices as well as additional enhancements. In May 2002, USPTO began transitioning PACR from PTONet to PTONet II, the upgraded USPTO-wide LAN.

In response to our earlier report, USPTO initiated a contractor-supported certification and accreditation[2] (C&A) pilot project for five of its critical systems. USPTO identified PACR as one of those systems after we began our evaluation. For each of the systems, the C&A pilot project will provide the following:

- risk assessment,
- updated security plan,
- vulnerability assessment,
- business continuity plan,

[1] Office of Inspector General. 2002. *Additional Senior Management Attention Needed To Strengthen USPTO's Information Security Program*, Final Inspection Report No. OSE-14816/March 2002. Washington, DC: Office of Inspector General U.S. Department of Commerce.

[2] Certification is the formal testing of the security safeguards implemented in a computer system to determine whether they meet applicable requirements and specifications. Accreditation is the formal authorization by management for system operation, including an explicit acceptance of risk.

- security test and evaluation (ST&E) plan, and
- certification and accreditation package.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our evaluation was to conduct an independent assessment of the implementation of information security controls for PACR. We used NIST's *Security Self-Assessment Guide for Information Technology Systems,*[3] as the basis for evaluating controls in three categories: management, operational, and technical. Because of resource and time constraints, we selected a subset of these controls for evaluation. Table 1 identifies the controls we chose to assess. We further reduced the set by eliminating technical controls because USPTO was unable to provide accurate, consistent information about the system and to avoid duplication of effort, since the pilot project will evaluate technical controls for PACR.

Table 1 Security Controls Selected for Assessing PACR

Control Category	Control	Selected
Management	Risk Management	X
	Review of Security Controls	X
	Life Cycle	X
	Authorize Processing	X
	System Security Plan	X
Operational	Personnel Security	
	Physical Security	X
	Production, Input/Output Controls	
	Contingency Planning	X
	Hardware and Systems Software Maintenance	
	Data Integrity	
	Documentation	
	Security Awareness, Training, and Education	X
	Incident Response Capability	
Technical	Identification and Authentication	X
	Logical Access Controls	X
	Audit Trails	X

During our evaluation, we reviewed PACR system documentation, conducted interviews with USPTO personnel and managers involved in PACR development and information security, and visited USPTO facilities where equipment to support PACR operations is located.

[3] National Institute of Standards and Technology. 2001. *Security Self-Assessment Guide for Information Technology Systems,* NIST Special Publication 800-26. Gaithersburg, MD: National Institute of Standards and Technology.

USPTO is already implementing the recommendations from our March 2002 review, which should address many of the problems found in this current review. For those concerns currently being addressed, we make no new recommendations.

Our evaluation was conducted in accordance with the Quality Standards for Inspections issued by the President's Council on Integrity and Efficiency and was performed under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated May 22, 1980, as amended. Our fieldwork was conducted from January through May 2002.

FINDINGS AND RECOMMENDATIONS

We found that physical security measures in place during our evaluation provide appropriate protection for equipment that PACR relies on to support USPTO operations. Our review further determined, however, that (1) management controls are not implemented and that both (2) contingency planning and (3) specialized security training are needed.

I. Physical Security Measures Are Generally Appropriate

The PACR servers that store images of patent applications, as well as the firewall that affords protection from unauthorized access to the servers, are located in a secure data center. Access to the data center is controlled by a personnel badge reader and an electronic key card reader. USPTO's Office of Information System Security effectively controls activation and deactivation of the badges and key cards. In addition, security personnel are on duty inside the data center 24 hours per day, 7 days per week. Visitors must be authorized access and must display proper identification while in the center, where they are escorted at all times. As an added control, surveillance cameras continuously monitor the database server and surrounding areas.

The scanning servers that create the patent application images are located in a building separate from the building that houses the secure data center. These servers are located in a secure room whose access is controlled by a cipher lock. Visitor access is controlled by a system administrator, who also monitors the operational status of the servers.

We noted during our evaluation that the cipher combination to the room is not changed after employees and contractors who have been given the combination terminate employment or contractual obligations with USPTO. In response to our concern, USPTO is developing an agency-wide policy for changing cipher combinations.

Further, USPTO plans to move the scanning servers from the secure room to the secure data center where the remaining servers and the firewall are housed.

Recommendation

We recommend that the Commissioner for Patents and the USPTO Chief Information Officer ensure that the agency establishes and implements a policy requiring that cipher combinations be changed (1) when employees and contractors who have the combinations depart USPTO service or no longer require access and (2) on a periodic basis.

II. Management Controls Are Not Implemented

Management controls focus on the management of the information technology security aspects of a system and the management of risk. For PACR, we found that management controls are not fully implemented for the following reasons:

- a risk assessment has not been conducted,
- the security plan is not approved,
- the operational system has not been accredited,
- security controls have not been tested and reviewed periodically, and
- life cycle management deficiencies exist.

A. Risk Assessment of PACR Has Not Been Conducted

A current risk assessment for a system is the foundation of a risk-based approach to information security because it is designed to identify threats and vulnerabilities so appropriate security measures can be implemented. GISRA requires program officials to determine and assess risks to the operations and assets they control, and OMB Circular A-130, Management of Federal Information Resources, requires agencies to use a risk-based approach to determine adequate security measures.

No risk assessment has been performed for any version of PACR; therefore, it is not possible to determine whether security measures are adequate to deal with existing threats and vulnerabilities. USPTO recognized this deficiency and tasked a contractor to conduct a risk assessment for the operational PACR system as part of the ongoing C&A pilot project.

B. Security Plan Is Not Approved

The Computer Security Act of 1987 requires that security plans be developed for all federal computer systems that contain sensitive information. A system security plan provides an overview of system security requirements and describes the controls in place or planned for meeting those requirements. It also delineates responsibilities and expected behavior of all individuals who access the system. Since the plan establishes the security controls, it should logically form the basis for accreditation of the system. The security plan should be reviewed annually and revised as needed to ensure that security controls can handle significant changes to the system and address rapidly changing threats.

At USPTO, the project manager is responsible for preparing and maintaining the information system security plan throughout the system's life cycle, with assistance from the information system security officer (ISSO).

Although security plans have been developed for PACR, USPTO was unable to provide official sign-off or approval pages or documented Technical Review Board[4] action to indicate that any of these plans have been officially approved. Hence, PACR lacks a critical component—an approved security plan—needed for accreditation. The most recent PACR security plan will be updated during the ongoing pilot project.

C. Security Controls Have Not Been Periodically Tested and Reviewed

OMB Circular A-130 requires that agencies perform a formal management review of security controls at least every 3 years. Such reviews should also be conducted when significant changes are made to a system. Reviews should include an independent assessment of security controls and can include network scans, analysis of network device settings, and penetration testing. Testing and reviewing security controls are critical factors for system accreditation.

Testing of security controls for PACR has not been performed. USPTO has tasked a contractor to conduct a vulnerability assessment for the operational PACR system as part of the pilot project. As part of the vulnerability assessment, the contractor will use a detailed questionnaire to assess the effectiveness of management, operational, and technical controls and will use a network scanner (CyberCop) provided by USPTO to determine the effectiveness of controls against known vulnerabilities. If this assessment is comprehensive and thorough, it should adequately test PACR security controls.

In response to our previous evaluation, USPTO is putting a process in place to periodically test and review security controls related to each system.

D. System Has Not Been Accredited

OMB Circular A-130 requires management officials to formally authorize the use of a system before it becomes operational and re-accredit the system whenever a significant change is made or at least every 3 years. By authorizing processing, a management official acknowledges an understanding and acceptance of the risks associated with putting the system into operation.

No version of PACR has been accredited as yet; however, USPTO and contractor personnel are preparing certification and accreditation materials, which will lead to accreditation of PACR, as part of the C&A pilot project.

[4] The Technical Review Board conducts reviews of work products and plans during the life cycle of an automated information system.

E. Life Cycle Management Deficiencies Found

Security Considerations of System Design Changes Are Not Well Planned

USPTO is currently making the transition from its local area network (LAN), PTONet, to PTONet II, a more capable LAN based on current network technology. The LAN allows USPTO users to communicate with servers, send and receive e-mail, execute applications, search for information, and support business processes. Because USPTO's LAN supports processing associated with patent applications, the transition will require changes to PACR network components and related software.

USPTO's PTONet II Production Installation Plan states that the transition for systems such as PACR would be planned well in advance, and meetings would be conducted with system development managers, other USPTO officials, and contractor managers responsible for PTONet II installation. These meetings were to address such issues as changing internet protocol addresses[5] for PACR network components to accommodate PTONet II. However, PACR system design changes to accommodate PTONet II do not appear to have been well planned, nor did they adequately consider network security implications. We reached these conclusions because, just prior to the initial transition step for PACR, USPTO was unable to identify required software changes and necessary modifications and additions to firewall rules. Furthermore, the ISSO was unaware that these changes were about to be made, even though the Office of Information System Security, which is under the direction of the ISSO, is responsible for reviewing and authorizing proposed firewall changes.

Draft procedures for implementing PACR network and firewall changes were issued after initial transition attempts failed. Since the completion of our fieldwork, the transition of PACR to PTONet II was successfully completed.

USPTO needs to better plan and coordinate information technology changes that affect security aspects of interconnected systems.

Documentation Does Not Reflect Current System

System documentation should be current and accurate to support testing, training, modification, and maintenance activities. The quality and utility of supporting documentation can be considered a primary measure of the health and well-being of a software project.[6]

To understand the network and security architecture of PACR, we reviewed available system documentation and attended briefings provided by USPTO. (As noted previously, USPTO had no record of an approved information security plan for PACR.) We found that:

- available documentation does not reflect the current system;
- network topology diagrams, four in all, have the same issuing date but each differs from the others and none accurately describes the then-current or planned topology; and

[5] An internet protocol (IP) address identifies a specific computer or device on a network.
[6] Fairley, R. 1985. *Software Engineering Concepts.* New York: McGraw-Hill , p. 220.

- for the High-level Architecture document and Operational Support Plan, discrepancies exist between their network topology diagrams, equipment lists, and points of contact.

USPTO needs to improve its process for keeping documentation current and tracking its status.

Recommendations

We recommend that the Commissioner for Patents and the USPTO Chief Information Officer make certain that agency managers ensure that:

1. PACR system documentation is updated to reflect the current operational system, and

2. a process to track document approval is established and enforced.

III. Contingency Planning Is Needed

OMB Circular A-130 states that managers should develop plans for how they will perform their mission and recover from the loss of system support. The circular also notes that testing a contingency plan significantly improves its viability, and plans that have not been tested, or have not been tested recently, may mask an agency's ability to recover in a timely manner.

PACR has no contingency plan, but USPTO is developing a Business Continuity Plan as part of the ongoing C&A pilot project.

IV. Specialized Security Training Is Needed

GISRA requires chief information officers to ensure the training of personnel who have significant responsibilities for information security. However, PACR system administrators have not received specialized security training. USPTO has agreed with our earlier recommendation to develop a comprehensive information security training and education program based on job functions, roles, and responsibilities using NIST Special Publication 800-16.[7] Thus, PACR system administrators should receive specialized training as this program is implemented.

[7] Information Technology Laboratory. 1998. *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. Gaithersburg, MD: U.S. Department of Commerce National Institute of Standards and Technology.

UNITED STATES
PATENT AND
TRADEMARK OFFICE

Attachment

Under Secretary of Commerce For Intellectual Property and
Director of the United States Patent and Trademark Office
Washington, DC 20231
www.uspto.gov

AUG 16 2002

MEMORANDUM FOR Judith J. Gordon
Assistant Inspector General for Systems Evaluation

FROM: Nicholas P. Godici
Commissioner for Patents

Douglas J. Bourgeois
Chief Information Officer

SUBJECT: Response to OIG Draft Inspection Report No. OSE-14926, Stronger Management Controls Needed for the Patent Application Capture and Review Automated Information System

The staff of the United States Patent and Trademark Office (USPTO) has reviewed the subject draft report and concurs with the Office of the Inspector General (OIG) findings. In the attachment, we provide a brief explanation of how we are implementing each recommendation.

We are continuing to work together to develop and implement an effective IT Security Program across the USPTO. This means that the activities described in the draft report have been added to the USPTO's Plan of Action and Milestones (POA&M) reported to OMB on a quarterly basis.

If you have any questions or wish to discuss any issues, please contact Susan Callis, IT Security Program Manager, at (703) 305-3898 or Susan.Callis@USPTO.gov.

Attachment

cc:
James Rogan, Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office
Jon W. Dudas, Deputy Under Secretary of Commerce for Intellectual Property and Deputy Director of the United States Patent and Trademark Office
James A. Toupin, General Counsel
Clarence C. Crawford, Chief Financial Officer and Chief Administrative Officer
Sandra L. Weisman, Deputy Chief Financial Officer and Comptroller
Anne Chasser, Commissioner for Trademarks

OIG Recommendations and
USPTO Action Plan

1. **The Commissioner for Patents and the USPTO Chief Information Officer ensure that the agency establishes and implements a policy requiring that cipher combinations be changed (1) when employees and contractors who have the combinations depart USPTO service or no longer require access and (2) on a periodic basis.**

Procedures have been developed and have been provided to the contractor maintaining the secure room where the PACR server is currently housed. This is the only room in the USPTO where cipher locks are currently used to secure IT equipment.

2. **The Commissioner for Patents and the USPTO Chief Information Officer make certain that agency managers ensure that:**

   a. **PACR system documentation is updated to reflect the current operational system, and**
   b. **A process to track document approval is established and enforced.**

The next software build for PACR, version 3.7 is in development. All PACR system documentation is being updated to reflect this version.

Procedures have been developed for the Change Management Control of IT Security documents, including signature pages indicating document approval. A meeting is scheduled for August 22 to discuss the feasibility of adopting these procedures for all system documentation.

The new OCIO Office of Information Systems Security Director, who joined the USPTO OCIO on August 12, will be establishing procedures for approving and controlling information system IT Security documentation. He will coordinate these procedures with the Directors of other appropriate offices to reach agreement on their applicability to other system documentation.

ATTACHMENT 1