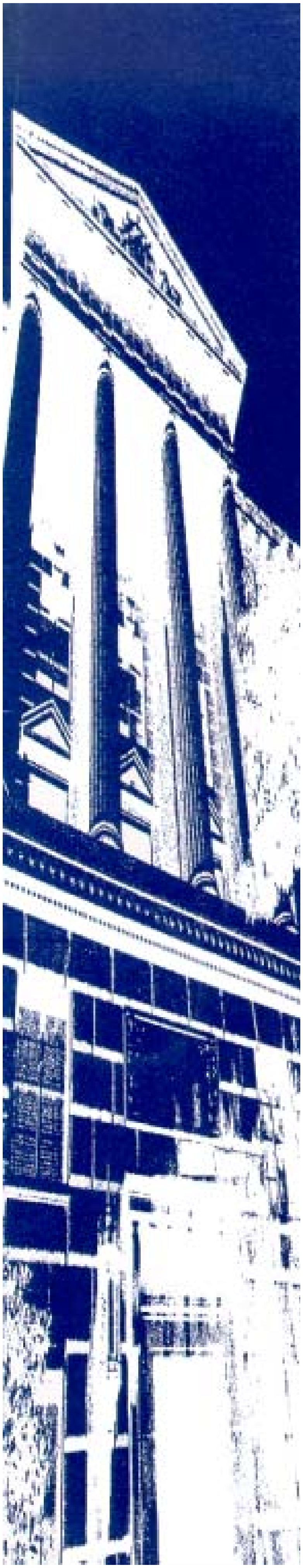
U.S. DEPARTMENT OF COMMERCE
Office of Inspector General



UNITED STATES PATENT AND TRADEMARK OFFICE

Additional Senior Management Attention Needed to Strengthen USPTO's Information Security Program

Final Inspection Report No. OSE-14816/March 2002

PUBLIC RELEASE

Office of Systems Evaluation

CONTENTS

EXECUTIVE SUMMARY

USPTO's day-to-day operations grow increasingly dependent on information technology—patent and trademark applications are filed, fees are paid, and some USPTO employees telework electronically via the Internet, just to cite a few. These advances promise to improve delivery of USPTO services, but they also increase the risk to and vulnerability of USPTO's computer systems and networks. Greater access escalates the risk of unauthorized access and exposure of USPTO's data to unauthorized disclosure or modification.

The objective of our evaluation was to determine whether USPTO's information security program for unclassified systems complies with the Government Information Security Reform Act (GISRA), which mandates that federal agencies have effective security for the information resources supporting their operations and assets. Using NIST's *Security Self-Assessment Guide for Information Technology Systems*,[1] as recommended by OMB, we evaluated USPTO's information security policies and procedures, roles and responsibilities, and adherence to applicable laws, regulations, and guidance.

Under GISRA, information security is the responsibility of agency senior management—the agency head, senior agency officials, and the Chief Information Officer (CIO). Each agency head is charged with ensuring the security of information and information systems by promoting security as an integral component of that agency's business operations.

We found that although USPTO generally has documented policies and procedures in place that are consistent with accepted security practices, many other important security requirements are not satisfied. Our findings suggest that information security has not yet become an integral part of USPTO's business operations; therefore, fundamental responsibilities are frequently not carried out. In its GISRA reporting to OMB for fiscal year 2001, we are concerned that USPTO substantially overestimated the quality of its security program and presented unrealistic expectations for improvement for this year and next. Moreover, it should be noted that we have identified strengthening information security as a top 10 management challenge for the Department. Although the American Inventors Protection Act of 1999 (P.L. 106-113) recast USPTO as a performance-oriented organization, giving it substantial autonomy and independence from the Department, this challenge applies to USPTO as well.

Our evaluation found the following issues:

- Eighty-two percent of USPTO's 78 operational systems do not have documented risk assessments, 30 percent of its security plans are outdated, and none of its operational systems have a current accreditation as required by OMB Circular A-130. Lack of accreditation means that USPTO management has not officially authorized any of these systems for use. Moreover, USPTO officials do not conduct periodic reviews of information policies and

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

security controls and techniques. As a result of these problems, USPTO lacks assurance that its operational systems are adequately protected. (See page 8.)

- USPTO provides information security-awareness training to new employees, but does not have a program to provide adequate training and education to personnel who need specialized security skills and competencies. Thus, USPTO cannot ensure that employees who have significant security responsibilities understand or apply effective information security practices. (See page 13.)

- USPTO's incident response procedures do not include any requirement to report incidents to the General Services Administration's Federal Computer Incident Response Center or to OIG. Such reporting is required by GISRA and OMB guidance. In addition, incident reporting is a valuable tool that aids the federal government in recognizing and detecting intrusions and securing its information systems. (See page 14.)

- USPTO's funding requests for information security do not appear to be based on a thorough analysis of its security needs or the cost of satisfying them. Even though OMB stated it will not approve funding for projects that do not include the cost of meeting security requirements, USPTO did not identify costs for these requirements in its fiscal year 2002 or 2003 budget submissions. If challenged by OMB, USPTO will not be able to justify the funding it requested to plan and implement needed security improvements. (See page 15.)

- Although essential to establishing the environment and ensuring the resources needed to promote an effective information security program, senior management's awareness and support of this program are minimal and its proactive involvement is absent. Because USPTO's information security needs have not received adequate attention by senior management, significant weaknesses exist in its information security planning, budgeting, implementation, review, and oversight. (See page 17.)

We made numerous recommendations for improving information security at USPTO (see pages 11, 12, 15, 16, and 18). Most importantly, we recommend that the Under Secretary of Commerce for Intellectual Property and Director of USPTO ensure that senior management officials give information security high priority, sufficient resources, and their personal attention and that they work closely with the CIO to improve information security at USPTO (see page 18).

…

USPTO agreed with all of our recommendations and has described corrective actions it is taking or has planned (see Attachment). We have included a synopsis of USPTO's response and, where appropriate, our comments on its response.

As regards accreditation, USPTO indicated that whether it can complete system accreditations according to the timetable we recommend depends on the resources required and their availability (see page 23). Because of the importance of accreditation in ensuring that operational systems are adequately protected, when allocating resources, we urge USPTO to give this matter high priority. USPTO also sought clarification on incident reporting procedures (page

25) and the acceptability of reporting incidents to the Department, which would then relay the information to FEDCIRC. The OIG accepts this as a suitable approach.

USPTO's response to the Draft Inspection Report is included as Attachment A.

INTRODUCTION

On October 30, 2000, the President signed into law the Government Information Security Reform Act (GISRA), Title X, subtitle G, of the 2001 Defense Authorization Act (P.L. 106-398). The law amends the Paperwork Reduction Act of 1995 by enacting a new subchapter on information security, which primarily addresses managing, implementing, overseeing, and ensuring the security of unclassified and national security information systems.

Under GISRA, information security is the responsibility of agency senior management—the agency head, senior line managers, and the Chief Information Officer (CIO). Appropriate senior officials are responsible for assessing security risks associated with operations and assets for the programs and systems over which they have control. Each agency head is charged with ensuring the security of information and information systems by promoting security as an integral component of that agency's business operations. Each is also charged with ensuring that an information security plan to safeguard the privacy, confidentiality, and security of federal information is carried out throughout the life of each system.

The agency CIO is required to administer the information security program agency-wide. This includes developing the security program, ensuring that the program is effectively implemented and maintained, training and overseeing personnel with significant responsibilities for information security, and assisting other senior agency officials with their information security responsibilities.

GISRA also requires all federal agencies to perform annual reviews of their security programs and the Office of Inspector General (OIG) for each agency to conduct independent evaluations. This report presents the results of our independent evaluation of the U.S. Patent and Trademark Office (USPTO) information security program as required by GISRA.

This draft report presents the results of our evaluation of USPTO's information security policies and procedures as they apply to USPTO entitywide. A separate report that OIG recently provided to USPTO presents a review of the adequacy and effectiveness of the general controls related to the integrity, confidentiality, and availability of information specifically associated with USPTO's financial systems, which is required as part of the audit of USPTO's financial statements.[2] A review of the security of selected non-financial information systems will be conducted separately.

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.

[2] US Department of Commerce, Office of Inspector General, February 2002. *Improvements Needed in the General Controls Associated with USPTO's Financial Management Systems,* Audit Report No. FSD-14477-2-0001. Washington, DC: US Department of Commerce..

BACKGROUND

At USPTO, information technology increasingly supports day-to-day operations. Greater reliance on the Internet is evidenced by the increasing numbers of clients electronically filing patent and trademark applications and paying fees and by the larger number of USPTO employees who use the Internet to communicate for purposes of teleworking. Although these advances promise to improve USPTO's ability to deliver services, they expose the agency's computer systems and networks to a greater risk of unauthorized access and increase the possibility of unauthorized disclosure or modification of USPTO data. Cost-effective security measures are required to protect USPTO's information assets.

USPTO's Allocation of Information Security Responsibilities

Many offices within USPTO have information security responsibilities (The shaded boxes in Figures 1 and 2 indicate the offices discussed in this report that share responsibility for information security.) Some key responsibilities are described here; other roles and responsibilities are presented in Appendix A.

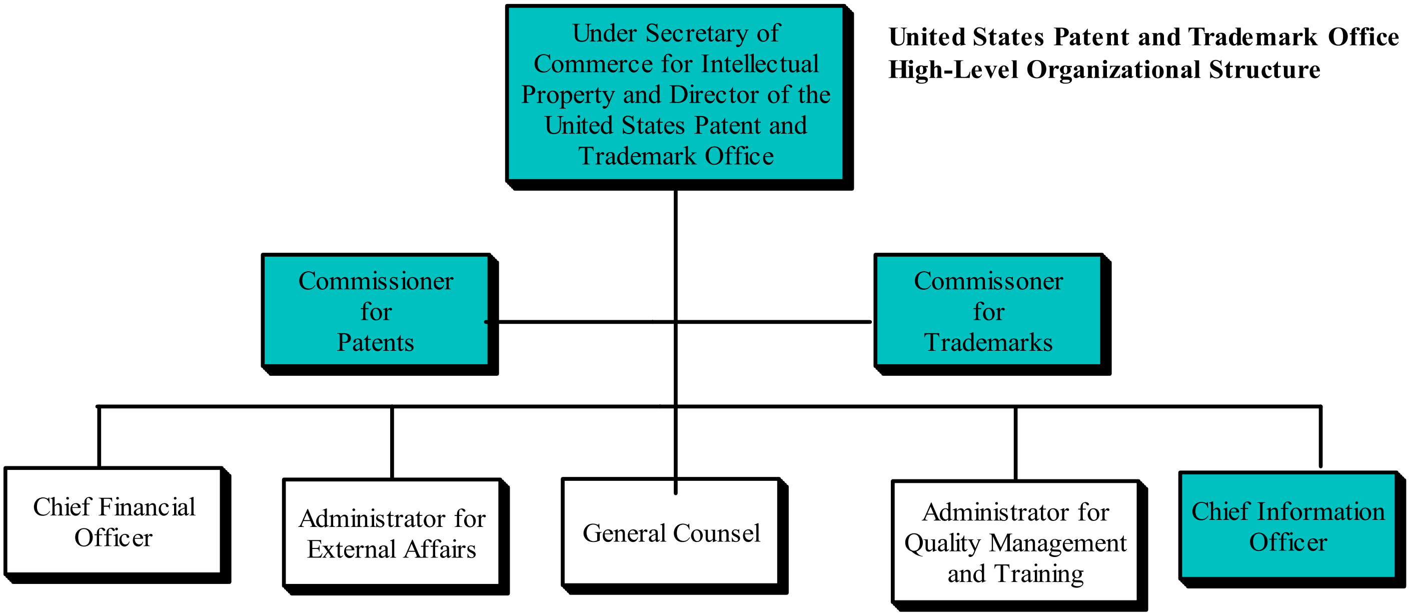

Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office
United States Patent and Trademark Office High-Level Organizational Structure
Commissioner for Patents
Commissoner for Trademarks
Chief Financial Officer
Administrator for External Affairs
General Counsel
Administrator for Quality Management and Training
Chief Information Officer

Figure 1. Responsibilities for Information Security

The Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office determines the policies, directs the programs, and is responsible for all activities of USPTO. The Under Secretary is also ultimately responsible for approving all information technology strategies and initiatives and has the overall responsibility of ensuring the confidentiality, integrity, and availability of information systems and assets.

The Commissioner for Patents provides administrative and policy direction to patent examining groups and related operations and validates functional requirements, including security requirements. The Commissioner for Trademarks has the same responsibilities with regard to trademark examination.

The USPTO CIO approves information security policies and procedures and also is the principal advisor to the Under Secretary on the application of information technology to support and improve USPTO business processes and information.

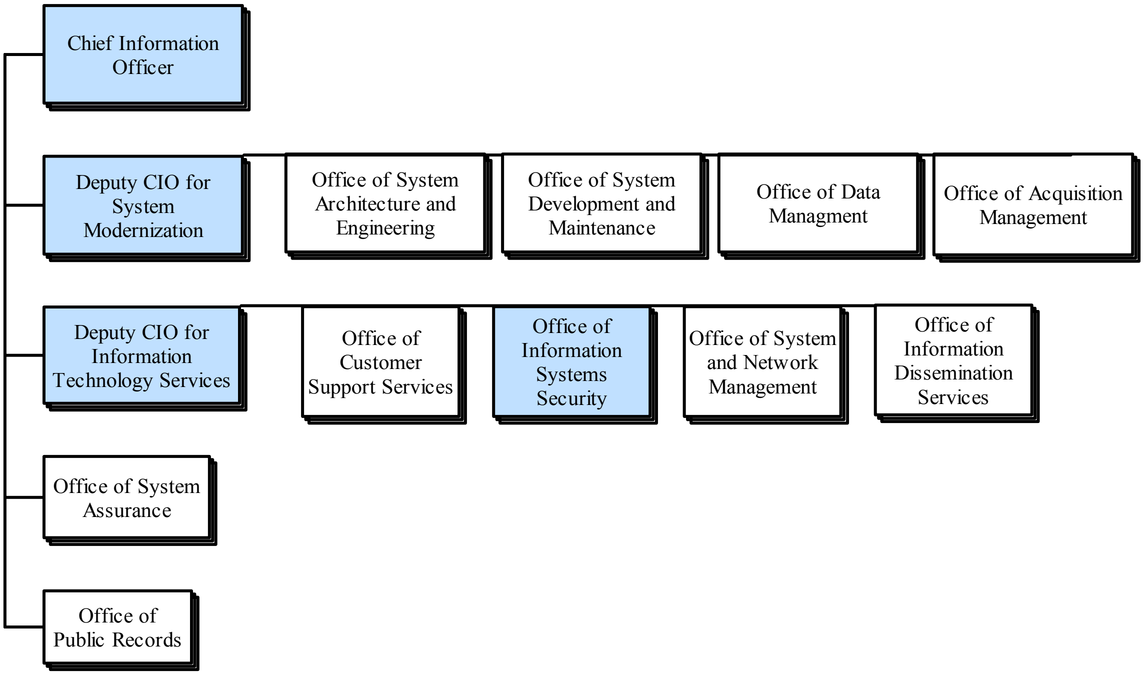

Chief Information Officer
Deputy CIO for System Modernization
Office of System Architecture and Engineering
Office of System Development and Maintenance
Office of Data Managment
Office of Acquisition Management
Deputy CIO for Information Technology Services
Office of Customer Support Services
Office of Information Systems Security
Office of System and Network Management
Office of Information Dissemination Services
Office of System Assurance
Office of Public Records

Figure 2. Office of the Chief Information Officer

The Deputy CIO for System Modernization provides the CIO with system support for system architecture and engineering and for system development and maintenance. This official is responsible for ensuring that security is designed into each information system. This is accomplished by assigning a system development manager from this organization to each system being developed or acquired.

The Deputy CIO for Information Technology Services provides support to the CIO in the areas of technical support services, system and network management, and information dissemination. This position also provides administrative and policy oversight for the Office of Information Systems Security (OISS).

The Information Systems Security Officer manages the OISS and provides for the implementation, operation, and maintenance of an enterprise-wide information technology infrastructure security program. This position is also responsible for

- providing computer security consulting services to USPTO organizations;
- providing support for computer security training for end users and developers;
- conducting informal or formal compliance audits regarding requirements of OMB Circular A-130, the Computer Security Act, and other policies and laws; and
- leading technical development projects regarding the building and maintenance of the USPTO computer security infrastructure.

The Information Systems Security Officer is also responsible for public key infrastructure implementation, operations, and maintenance.[3]

USPTO's Fiscal Year 2001 GISRA Reporting

As noted previously, GISRA requires annual agency security program reviews in addition to annual OIG independent evaluations. As a result of the greater independence and flexibility allowed USPTO by the American Inventors Protection Act of 1999 (P.L. 106-113), USPTO submitted its fiscal year 2001 information security review separate from the Department's. In conducting its fiscal year 2001 review, USPTO used NIST's *Security Self-Assessment Guide for Information Technology Systems*,[4] (see Table 1 for control areas), which was recommended by OMB. The NIST guide builds on the Federal Information Technology Security Assessment Framework (Framework),[5] which provides agency officials with a method for determining the current status of their security programs relative to existing policy and, where necessary, establishing a target for improvement. The Framework establishes five levels of information security program effectiveness (Figure 3). Each level identifies the implementation steps that must be taken to achieve that particular assessment level.

Based on its self-assessment, USPTO reported that tested and reviewed information security procedures and controls were in place for all of its systems. That is, USPTO rated itself at level 4 under the Framework, stating, "With current funding levels, USPTO will meet 75 percent of level 5 compliance of GISRA at the end of FY 2002. However, we expect to achieve 100 percent compliance by the end of FY 2003."

[3] A public key infrastructure enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

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

[5] The framework is Appendix C of the NIST Security Self-Assessment Guide.

Table 1. NIST Security Control Areas

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

Level 1	Documented Policy
Level 2	Documented Procedures
Level 3	Implemented Procedures and Controls
Level 4	Tested and Reviewed Procedures and Controls
Level 5	Fully Integrated Procedures and Controls

Figure 3. Federal IT Security Assessment Framework

In reviewing the information supporting the self-assessment, we found that USPTO merited an overall score of no more than level 2, and our independent evaluation results, presented in this report, confirm this lower rating. Thus, our evaluation shows that in its reporting to OMB, USPTO substantially overestimated the quality of its fiscal year 2001 security program and presented an expectation for 2002 and 2003 that is far from realistic.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this evaluation was to determine whether USPTO's information security program for unclassified systems complies with GISRA, which seeks to achieve effective security for information resources supporting federal operations and assets. We satisfied this objective by evaluating USPTO's information security policies and procedures, roles and responsibilities, and adherence to applicable laws, regulations, and guidance. A review of selected information systems will be conducted separately.

We reviewed USPTO's information security policies and procedures using criteria in NIST's Security Self-Assessment Guide and the Federal IT Security Assessment Framework cited above. The Framework establishes five levels (Figure 3) of security effectiveness and covers the three major control areas identified by NIST (Table 1). We also used as criteria OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources; the Computer Security Act of 1987; and GISRA.

In addition, we reviewed USPTO's self-assessments of information systems and security controls that comprised its fiscal year 2001 GISRA submission, as well as its Strategic Information Technology Plan for fiscal years 2001-2006. We interviewed USPTO officials including the CIO, the Deputy CIO for Information Technology Services, the Acting Director for the Technical Plans and Policy Staff, the Acting Information Systems Security Officer, and the Director of the Office of Systems and Network Management.

We held an entrance conference with USPTO on February 11, 2001. Our fieldwork was conducted from October through December 2001. On February 1, 2002, we met with the CIO and members of his staff to discuss the results of our evaluation. These officials generally agreed with our findings and discussed steps that they are taking or have planned to improve information security at USPTO. These steps include:

- **Certification and accreditation.**[6] The CIO is obtaining contractor support to refine and finalize the certification and accreditation process, train USPTO personnel to use the process, and apply it to USPTO systems and networks.

- **Office of Information Systems Security.** The CIO is planning a reorganization of this office designed to improve security by separating responsibilities for security policy compliance from security operations.

- **Security Technology Working Group.** The CIO has established a security working group whose objectives are to develop information security technical and policy expertise and apply it to systems and infrastructure projects, to select security standards and products, and to implement security from an enterprise perspective.

[6] 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.

- **Identification of specific internal security weaknesses.** The CIO is obtaining contractor support to perform firewall zone vulnerability scans, assess computer virus protection, and recommend improvements.

These steps address a number of the issues we identified in our evaluation and, when implemented, should help to improve the security of USPTO information assets.

FINDINGS AND RECOMMENDATIONS

I. Information Security Policies and Procedures Are Formal and Documented

Key to managing information security is establishing and implementing formal, documented security policies—the primary mechanism by which management communicates its views and requirements and establishes cost-effective organizational and system security controls. A sound policy delineates the security management structure, clearly assigns security responsibility, and lays the foundation necessary to reliably measure progress and compliance.

USPTO's Technical Standards and Guidelines (TSG) Program includes formal and documented security policies and procedures. Two TSGs form the foundation of USPTO's information systems security program: (1) Automated Information System Security Planning, Technical Standard and Guideline USPTO IT-212.2-08 (August 2000) and (2) Automated Information System Security Controls Manual, Technical Standard and Guideline USPTO IT-212.2-15, (September 2000). These documents cover the three NIST-identified major areas of control: management, operational, and technical (Table 1). The policies and procedures the TSGs prescribe are consistent with accepted practices and generally adhere to applicable laws, regulations, and guidance governing information systems security.

We did, however, find one omission: there is no provision in the policy for identifying information security deficiencies that may potentially be a material weakness, in accordance with OMB Circular A-123, *Management Accountability and Control*, and the Federal Manager's Financial Integrity Act (FMFIA) and for bringing such deficiencies to the attention of the Department, as required by Department guidance. Failure to identify significant information security deficiencies results in sustained vulnerability and prolonged risk. (This topic is discussed further in Finding II.)

II. Key Management Controls Are Not Fully Implemented

Despite the fact that USPTO has formal documented policies, key management controls are not fully implemented: required risk assessments have not been completed, security plans are outdated, and management has not accredited operational systems, accreditation being the formal authorization by management for operational use.

A. Risk Assessments Have Not Been Completed

GISRA requires program officials to determine and assess the risks to the operations and assets over which they have control. OMB Circular A-130 no longer requires agencies to prepare formal risk analyses but does require them to use a risk-based approach to determine adequate security. This means security must be commensurate with the risk and magnitude of potential harm resulting from the loss, misuse, or unauthorized access to or modification of information. Risk assessments should incorporate the major factors in risk management: value of the system or application, possible costs of enacted threats or exploited vulnerabilities, and the effectiveness of current or proposed safeguards. Assessing risk to a system is an ongoing necessity, ensuring that new threats and vulnerabilities are identified so appropriate security measures can be implemented.

According to USPTO's Automated Information System (AIS) Security Planning TSG, the Information System Security Officer in coordination with the System Development Manager, is responsible for performing or contracting for risk assessments for USPTO’s information systems. The TSG also provides guidance and a sample template for preparing risk assessments.

We found that there are no documented risk assessments for 64 of USPTO’s 78 operational systems, fully 82 percent. Without risk assessments, USPTO cannot comprehensively analyze risks to its operational systems and therefore lacks a basis for determining what the appropriate security controls should be.

B. Security Plans Are Outdated

A system security plan provides an overview of the security requirements of the system 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. The security plan should be reviewed annually and revised as needed to ensure that security controls can handle significant changes to the system as well as rapidly changing threats.

At USPTO, the project manager, who represents the business area that will use the system, 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. USPTO's AIS Security Planning TSG contains procedures and a template for preparing these plans.

We found that 30 percent of USPTO’s security plans (representing 24 systems) were more than 3 years old. One of the systems is PTOnet, one of USPTO’s major systems. It supports office automation services and provides access to business applications and databases for more than 8,000 employees. It has undergone significant changes over the years, yet its security plan has not been updated since 1992. Without up-to-date security plans, USPTO has no assurance that current security controls provide adequate protection.

C. Systems Are Not Accredited

OMB Circular A-130 requires management officials to formally authorize the use of a system before it becomes operational. This authorization, also referred to as accreditation, denotes that the manager understands and accepts the responsibility for the risks associated with putting the system into operation. The authorization is based on an assessment of the management, operational, and technical controls. Because the security plan establishes and documents the system protection requirements and the security controls in place, it forms the basis for management's decision to authorize processing. A system should be re-authorized following any significant change or at least every 3 years. It should be done more often where risk and potential magnitude of harm are high.

At USPTO, accreditation is a group responsibility. The Project Manager, System Development Manager, and Information System Security Officer are responsible for preparing and submitting an accreditation package that includes a statement certifying that security controls, features, and procedures are activated and working as required. The CIO and the program sponsor have approval authority for accreditation and determine whether system controls are adequate and level of risk is acceptable based on an evaluation of this package. The AIS Security Planning TSG provides guidance on preparing the certification and accreditation package.

We found that none of USPTO's operational systems had a current authorization to process (accreditation). Although its Strategic Information Technology Plan, published in March 2001, established a milestone of accrediting all business-critical information systems by July 2005, USPTO has made little progress in reaching this milestone. The lack of accreditation indicates that management has neither formally reviewed the controls nor explicitly accepted the associated risk. As a result, USPTO lacks assurance that its operational systems are adequately protected. We therefore believe that USPTO needs to focus on and accelerate this milestone. It should prioritize its systems according to risk and importance, accredit the high-risk systems by the end of fiscal year 2002, and accredit all remaining systems by the end of fiscal year 2003.

D. Information Policies and Security Controls Are Not Periodically Reviewed

A system's security degrades over time as technology evolves and as personnel, procedures, and system locations change. Reviews should assure that policies and security controls are functioning effectively. OMB Circular A-130 requires that agencies perform a formal management review of controls at least every 3 years. Management authorization to process is based on a review of these controls.

The Office of Information System Security is responsible for reviewing and verifying, through test and evaluation, that the security controls, features, and procedures are in place and working as required before a system is accredited. The results of that review and verification are used as supporting documentation to continue accreditation. However, USPTO noted in its self-assessments that these reviews were not performed, citing funding constraints as the reason. Without these reviews, USPTO cannot ensure that security controls are appropriate and accomplish the intended purpose.

E. USPTO Needs to Determine Whether It Has a Potential Material Weakness

OMB Circular A-130 instructs agencies to identify security deficiencies pursuant to OMB Circular A-123 if during the reviews it is determined that there is no assignment of security responsibility, no security plan, or no accreditation. The agency's decision whether to report a material weakness should depend on the risk and magnitude of harm that could result from the weakness. As noted in the previous section, failure to report significant information security weaknesses could result in unaddressed, unacceptably high security risks.

As previously discussed, and illustrated in Figure 4, USPTO lacks up-to-date security plans and current accreditations for its operational systems. It needs to determine whether these deficiencies are potential material weaknesses to be brought to the attention of the Department, which would then make a determination of whether they are significant enough to be reported to the President and the Congress. Additionally, USPTO should revise its information security policy to identify information security deficiencies that are potential material weaknesses pursuant to OMB Circular A-123 and FMFIA, and bring them to the attention of the Department.

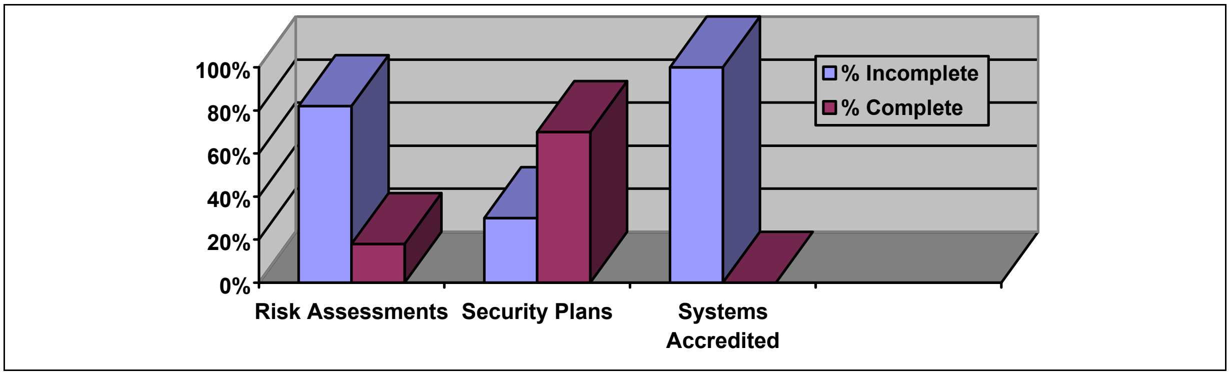


Figure 4. Status of USPTO's Key Information Security Management Controls

Recommendations

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office ensure that PTO managers take the following actions:

1. Conduct, document, and keep current, risk assessments for all operational systems.

   USPTO has agreed with this recommendation and has contracted with a vendor to develop procedures for certification and accreditation as well as perform these procedures on a pilot group of USPTO's most critical systems.

2. Develop up-to-date security plans for all operational systems.

   USPTO has agreed with this recommendation and has established a schedule for developing or updating security plans for all its operational systems. USPTO has noted that significant progress has been made and that approximately 80% of their operational systems now have current security plans.

3. (a) Prioritize all operational systems according to risk and importance, (b) accredit all high-risk systems by the end of fiscal year 2002, and (c) accredit all remaining systems by the end of fiscal year 2003.

   USPTO has agreed with this recommendation; however, its response indicates that completing system accreditations according to the timetable we recommend will depend on resource requirements and availability. Because of the importance of accreditation in

ensuring that operational systems are adequately protected, we urge USPTO to give this matter high priority when allocating resources.

4. Update accreditations at least every 3 years or whenever a significant change in the system occurs for all operational systems.

   USPTO has agreed with this recommendation and will be updating the IT Security Program Plan to include certifying and accrediting one-third of its AISs and infrastructure systems each year after FY 2003.

5. Implement a program stipulating periodic reviews and evaluations of the effectiveness of information security controls.

   USPTO has agreed with this recommendation. As part of the certification and accreditation process, USPTO will review and evaluate the security controls related to each system. USPTO will also annually out-source assessments of the infrastructure and other operational systems.

6. Revise USPTO's information security policy to include identifying information security deficiencies that may potentially be a material weakness pursuant to OMB Circular A-123 and FMFIA and bringing such deficiencies to the attention of the Department.

   USPTO has agreed with this recommendation and will develop an administrative order that defines the process for identifying and reporting material weaknesses to the Department.

III. Key Operational Controls Are Not Fully Implemented

USPTO's information security awareness, training, and education program and incident response capability are incomplete. As regards training specifically, USPTO needs to provide security awareness refresher training and training in relevant and needed security skills and competency for functional specialists and information security staff. Regarding incident response, USPTO's procedures must incorporate a reporting function that inculcates the sharing of information with relevant federal agencies.

A. Information Security Awareness, Training, and Education Are Inadequate

Information Security Awareness Requires Periodic Refreshing

USPTO's information security awareness program consists of new employee awareness training and published security awareness material. All new employees, as part of their orientation, receive a briefing by the Office of Information Systems Security on the proper and ethical use of USPTO's electronic information resources. In addition, USPTO has published two end user guides, *Rules of the Road Services Guide* and *Computer Housekeeping Guide*, which cover such topics as virus protection, data security, rules of behavior, and handling sensitive data.

Thus USPTO's information security awareness program covers the areas identified by OMB Circular A-130 and other applicable guidance governing security awareness; however, awareness training is a one-time occurrence and only for new employees. Follow-on security awareness information is provided via the static log-on screen-warning banner with references to the *Rules of the Road Services Guide*. OMB Circular A-130 notes that attention to security tends to dissipate over time. NIST states that a stimulus used repeatedly will eventually be selectively ignored. Therefore, USPTO should provide periodic refresher training to all employees to assure that they continue to understand and abide by the applicable rules.

Information Security Training and Education Program Needs to Be Developed

Under the Computer Security Act, each agency is required to provide mandatory periodic training in computer security awareness and accepted computer practices for all employees involved with the management, use, or operation of each federal computer system within or under the supervision of that agency. OMB Circular A-130 emphasizes these mandatory training requirements and further requires that prior to being granted access to applications and information systems, all individuals must receive specialized training focusing on their information security responsibilities and established system rules. In addition, GISRA requires that the agency CIO ensure the training of personnel who have significant responsibilities for information security.

USPTO's computer security training program consists of only information security awareness, which does not satisfy the supplementary training and education requirements. According to NIST, a formal information security training and education program focuses on providing the knowledge, skills, and abilities specific to an individual's roles and responsibilities relative to information systems.

Although information security officers and other employees with security responsibilities receive some relevant training, that training is not sufficient, and USPTO lacks a formal training program to ensure that employees receive security training applicable to their job function. Without such a program, USPTO cannot ensure that its security professionals and other employees with security responsibilities understand and apply information security practices effectively. USPTO needs to establish a formal information security training program aimed at ensuring that all personnel with significant security responsibilities understand information security risks and their responsibilities. NIST Special Publication 800-16 provides guidance on information security training requirements. These training requirements were derived from the information security program requirements established in OMB Circular A-130.

B. Incident Response Reporting And Handling Procedures Need To Be Revised

OMB Circular A-130 requires agencies to establish formal incident response mechanisms dedicated to evaluating and responding to security incidents in a manner that protects their own information and that of others who might be affected by the incident. The requirement stipulates that policies and procedures be documented and unnecessary internal obstacles to the timely reporting of incidents to the appropriate authorities be removed. The intent of the incident handling provision is to ensure that each agency has both the technical and procedural means in place to detect and appropriately report security incidents and share information on common vulnerabilities.

GISRA expands on the existing incident reporting policy by requiring agencies to notify and consult with law enforcement officials, other offices and authorities, and the General Services Administration's Federal Computer Incident Response Center (FedCIRC). OMB's implementation guidance for GISRA states that policies and procedures should facilitate the timely reporting to appropriate authorities within the agency, citing security officials and Inspectors General as examples. Reporting of incidents not only is required, but increased sharing of information concerning attempted intrusions, threats, and common vulnerabilities among organizations has been identified by GAO and FedCIRC as a valuable tool the federal government as a whole can use to identify and assist in detecting intrusions and securing federal information systems. An important aspect of information sharing is reporting to FedCIRC any event violating an explicit or implied security policy. FedCIRC requires that agencies establish points of contact to facilitate the reporting of incidents and the receipt of warnings and alerts from FedCIRC.

We found that USPTO's documentation of information security incident response procedures is consistent with OMB Circular A-130. The documents appropriately identify roles and responsibilities, define incident types and severity levels, and have reporting requirements. However, USPTO does not require the Information Systems Security Officer to notify or consult with OIG and external security offices and authorities in accordance with OMB guidance. For the period from October 2000 to October 2001, USPTO internally recorded several high-severity information security incidents, but did not report any to FedCIRC or OIG.

USPTO is aware that its current incident handling and reporting procedures do not meet GISRA requirements and has drafted a new set of procedures to meet these requirements. USPTO needs to ensure that these procedures address the reporting of incidents to FedCIRC and to DOC OIG.

Recommendations

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office ensure that USPTO managers take the following actions:

1. Provide information security awareness refresher training periodically to all employees.

   USPTO has agreed with this recommendation. A joint program office working group was established and has developed IT security user training awareness material that will be provided to all USPTO employees in the next 2 months.

2. Develop and implement, using NIST Special Publication 800-16 as a guide, a comprehensive information security training and education program based on job functions, roles, and responsibilities.

   USPTO has agreed with this recommendation and has plans to develop a comprehensive IT security training program using the NIST guidelines.

3. Track, on an annual basis, the number of employees trained and the type and cost of training provided.

   USPTO has agreed with this recommendation and is working to create a database to track personnel who have completed IT security training.

4. Revise incident reporting procedures to incorporate notifying DOC OIG and FedCIRC

   USPTO has agreed with this recommendation and is updating its incident reporting procedures. USPTO has indicated that the Department has requested that incidents be reported to them and that they will relay the information to FedCIRC. The OIG accepts this as a suitable approach.

IV. Information Security Requirements Should Be Identified in Capital Asset Plans and Linked to Security Cost Estimates

Under GISRA, agencies must identify and budget for security measures and resources needed to protect IT investments, starting from the earliest planning stages and throughout the investment life cycle. According to OMB Circular A-11, which governs preparing and submitting budget estimates, security costs are to be presented as a percentage of the total system cost or project investment in Exhibit 53, “Agency IT Investment Portfolio”; and capital asset plans must be provided (Exhibit 300), indicating whether the project’s security meets GISRA requirements and describing the security and privacy measures to be used.

Despite GISRA requirements and the statement from OMB that it will not approve funding for projects that do not include costs for meeting system-specific security needs, USPTO did not identify security costs for any individual system in its fiscal year 2002 or 2003 budget submissions. Even if a security funding request had been included, the amount would have been questionable because USPTO has not conducted an accurate, thorough analysis of current security needs or the cost of satisfying them. Furthermore, fiscal year 2002-2007 budget formulation guidance provided by USPTO's Office of the Chief Information Officer does not contain instructions for incorporating security costs into budget formulations.

A lack of support within USPTO for information security funding has been cited as the reason for deficiencies in such areas as system accreditations and training. We believe that poorly substantiated budget requests have contributed to this problem. Without sound analysis, USPTO will not be able to justify funding that will be needed to plan and implement required security improvements. Indeed, most of the improvements we observed occurred not as a result of proactive analysis and planning, but as a direct response to an OIG audit or evaluation or to specific incidents.

Recommendations

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office ensure that USPTO managers take the following actions:

1. Revise USPTO's budget guidance to include analyzing and presenting information security costs and ensure that such costs are well substantiated.

   USPTO has agreed with this recommendation and is formulating additional budget guidance.

2. Explicitly identify information security requirements and costs on a system-specific basis in funding requests to OMB.

   USPTO has agreed with this recommendation and is refining its budget estimates at the system level for future submissions.

V. Information Security Could Be Improved by Proactive Attention from Senior Management

GISRA requires that the head of each agency ensure that the agency's information systems' security plans are carried out throughout the life cycle of each system to safeguard the privacy, confidentiality, and security of federal information. The agency head is also responsible for promoting security as an integral component of that agency's business operations; agency managers and program officials are to ensure that effective security policies and procedures are implemented throughout the life cycle of every IT system. As the foregoing discussion documents, information security has yet to become an integral component of USPTO's business operations. Thus, there is a lack of follow through in carrying out fundamental responsibilities, including

- identifying, assessing, and understanding risks to USPTO's IT assets;
- determining security needs commensurate with the levels of risk;
- planning, implementing, and testing controls that adequately address risk;
- promoting continued awareness of information security risk and providing appropriate training;
- continually monitoring and evaluating policy and effectiveness of information security practices; and
- integrating security into its capital planning and investment control process.

Our evaluation demonstrates that information security has not received adequate attention at USPTO and that significant weaknesses exist in planning, budgeting, implementation, review, and oversight of this area. Information security weaknesses throughout Commerce prompted OIG to identify strengthening information security as one of the Department's top 10 management challenges. Recognizing the severity of this issue, the Secretary of Commerce issued a memorandum to secretarial officers and heads of operating units in July 2001 stating that information security should be given high priority and sufficient resources and that these officials are expected to personally invest the time necessary to assure information security improvements (Appendix B). The memorandum directed these officials to work closely with and support their operating unit CIOs with respect to information security and to allocate sufficient resources at the operating unit level necessary for the protection of Commerce data and systems. This direction, however, was provided in the context of a departmental IT management restructuring, and the memorandum was not sent to the head of USPTO. Because strengthening information security is a top management challenge that is directly applicable to USPTO, the memorandum is relevant to USPTO.

The awareness, support, and proactive involvement of USPTO's senior management are, however, essential to establishing the environment and ensuring the resources needed to promote an effective information security program. We urge the Under Secretary of Commerce for

Intellectual Property and Director of USPTO to make improving the information security program a high priority and to direct USPTO senior management officials to do the same. He should ensure that these officials fully understand their information security responsibilities and make certain that sufficient resources are allocated to this essential area.

Recommendations

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office ensure that senior USPTO management officials:

1. Give information security high priority, sufficient resources, and their personal attention.

   USPTO has agreed with this recommendation. The USPTO Chief Information Officer and the Under Secretary of Commerce for Intellectual Property and Director will continue to work together to ensure that appropriate attention and resources are allocated to the IT Security Program. In addition, the USPTO Chief Information Officer will update the Executive Committee every 2 months at its regular meeting.

2. Work closely with the USPTO CIO to improve information security.

   USPTO has agreed with this recommendation and has appointed an interim IT Security Program Manager until the Office of Information Security is reorganized and IT security vacancies filled.

3. Be provided with explicitly defined and documented information security responsibilities.

   USPTO has agreed with this recommendation and a new administrative order will define information security responsibilities across USPTO.

APPENDIX A

2 Pages

Additional Information Security Roles Within USPTO[7]

Automated Information System (AIS) Security Analyst - assists the Project Manager in determining specific legislative, procedural, security, and confidentiality requirements for the AIS.

AIS Security Officer - assists the Project Manager with preparing the security information that is in the Operational Support Plan.

Director, Office of System Product Assurance - conducts independent tests of AIS system contingency plans and the Information Technology Infrastructure Disaster Recovery Plan.

USPTO Business Area Program Sponsor - ensures, with the assistance of the CIO, that information systems process and handle sensitive information in a cost-effective manner.

AIS Production Manager - appointed by the Business Area Program Sponsor, the Production Manager is responsible for the security of the AIS and serves as the AIS Security Officer for systems in operation.

AIS Project Manager - appointed by the Business Area Program Sponsor, the AIS Project Manager with the assistance of a System Development Manager conducts AIS sensitivity assessment, prepares the AIS Security Plan, identifies and prioritizes AIS security requirements, incorporates security training requirements in AIS training plan, serves as AIS Security Officer until Business Area Program Sponsor appoints a Production Manager or another business area employee to serve in the role, ensures that funding is available, and obtains contractor support to conduct the risk assessment.

System Development Manager - appointed by the CIO, the System Development Manager is responsible for designing, developing and deploying an AIS under the business direction of the Project Manager; also, works with the Information Systems Security Officer to ensure that adequate application controls are built into the AIS.

Office of Information Systems Security (OISS) Duty Officer - serves as a single point of contact on a rotational basis for user ID issues and other routine security issues, coordinates incident response activities.

Contracting Officer Technical Representatives - coordinates with Task Order Manager(s) for all security duties, initiates background check for contractors performing system administration.

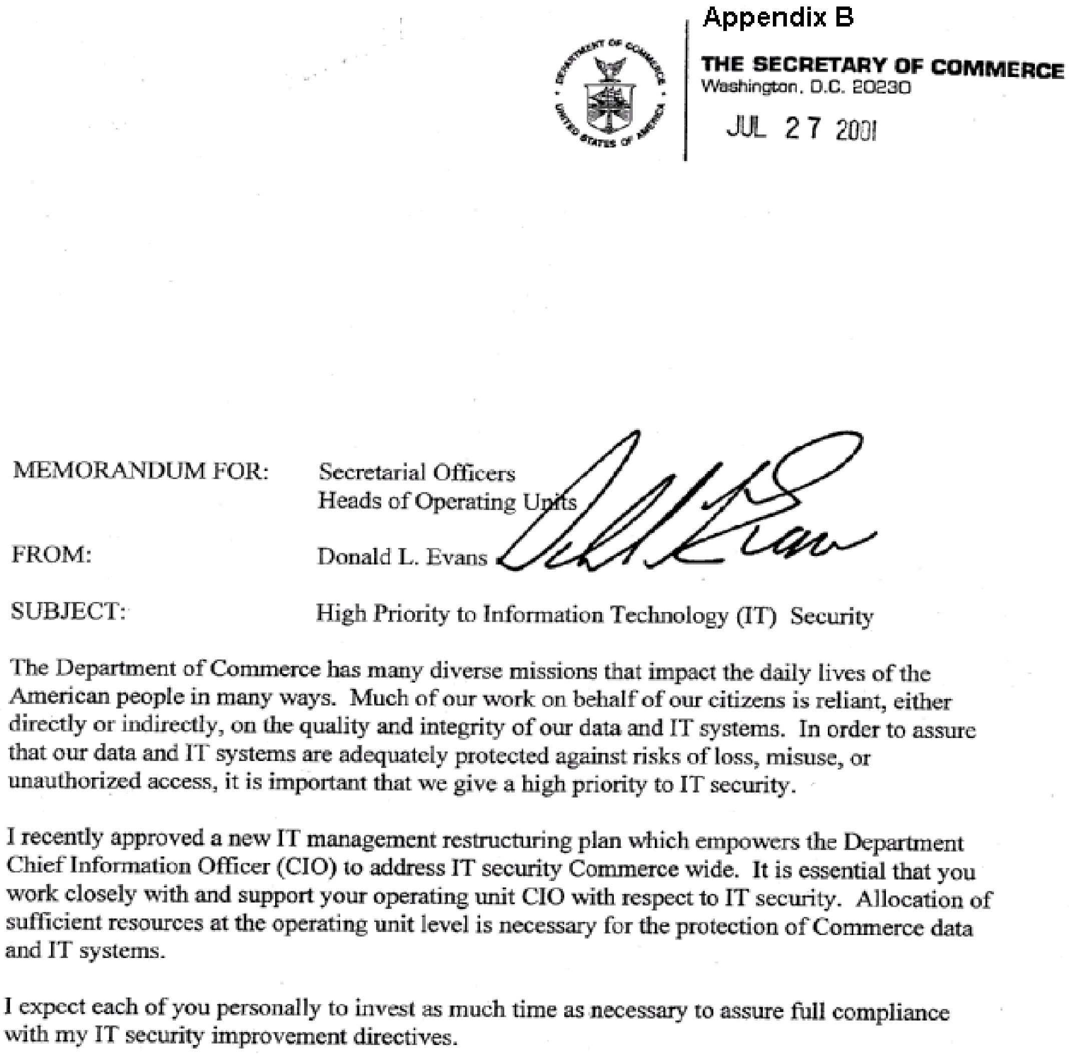
[7] US Patent and Trademark Office. *USPTO Automated Information System Security Control Manual, Technical Standard and Guideline,* USPTO IT-212.2-15. Washington, DC: US Patent and Trademark Office.

Office of System and Network Management - establishes and monitors operating system and hardware baseline information, reviews system logs, and reports anomalies to Office of Information Systems Security.

USPTO's Office of Security - performs national agency check, conducting inquiries regarding employees and contractors as required by federal policies and position determination.

Office of Human Resources - designates, with the assistance of the managers, the sensitivity or risk levels of positions in the operating unit; sends a list of departing USPTO personnel to the Office of Information Systems Security and the Office of System and Network Management; notifies the Office of System and Network Management and the Office of Information Systems Security of any personnel issues that may have a direct or indirect affect to information security.

APPENDIX B



Appendix B

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

JUL 27 2001

MEMORANDUM FOR: Secretarial Officers
Heads of Operating Units

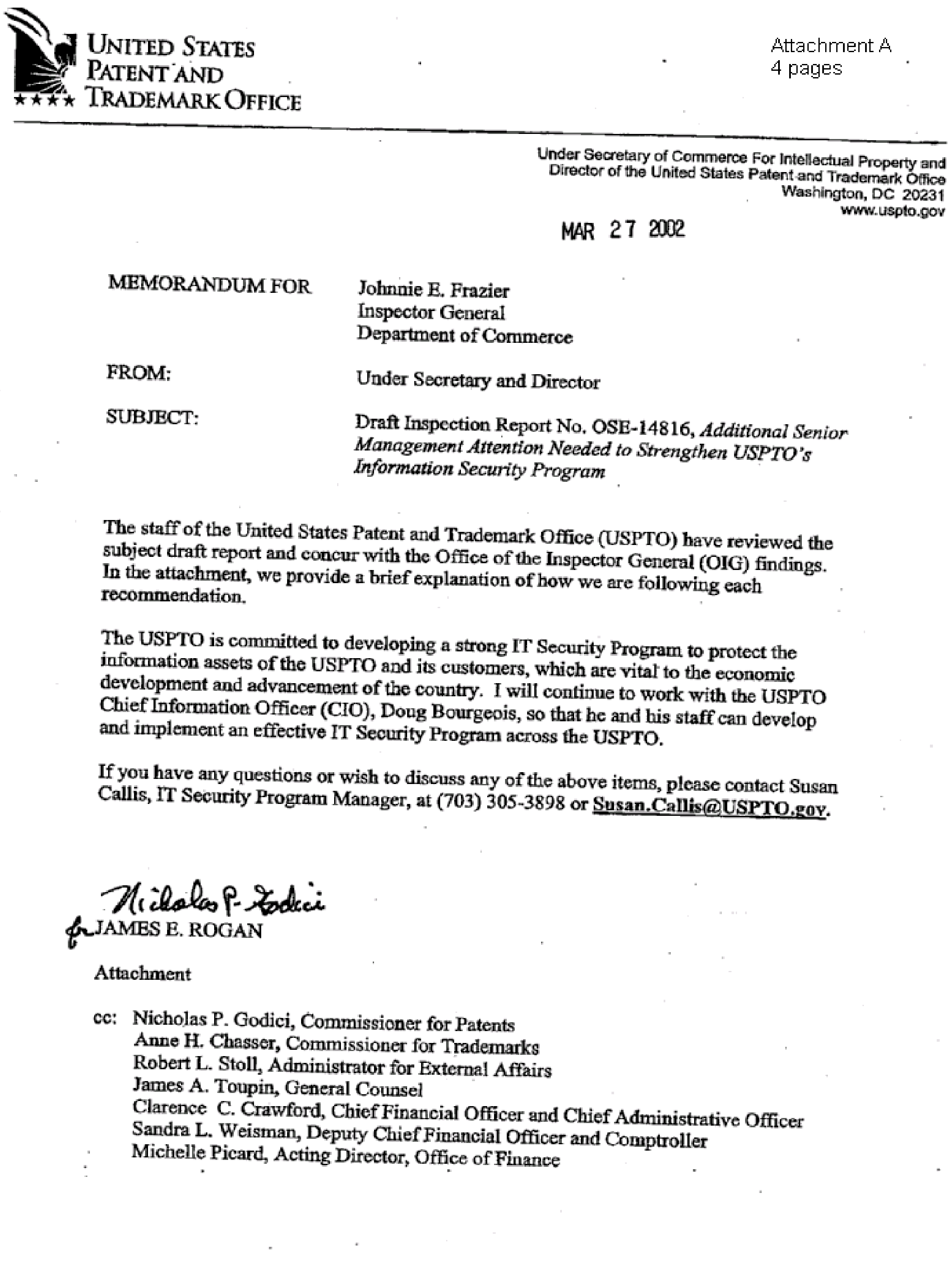
FROM: Donald L. Evans

SUBJECT: High Priority to Information Technology (IT) Security

The Department of Commerce has many diverse missions that impact the daily lives of the American people in many ways. Much of our work on behalf of our citizens is reliant, either directly or indirectly, on the quality and integrity of our data and IT systems. In order to assure that our data and IT systems are adequately protected against risks of loss, misuse, or unauthorized access, it is important that we give a high priority to IT security.

I recently approved a new IT management restructuring plan which empowers the Department Chief Information Officer (CIO) to address IT security Commerce wide. It is essential that you work closely with and support your operating unit CIO with respect to IT security. Allocation of sufficient resources at the operating unit level is necessary for the protection of Commerce data and IT systems.

I expect each of you personally to invest as much time as necessary to assure full compliance with my IT security improvement directives.



UNITED STATES
PATENT AND
TRADEMARK OFFICE

Attachment A
4 pages

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

MAR 27 2002

MEMORANDUM FOR Johnnie E. Frazier
Inspector General
Department of Commerce

FROM: Under Secretary and Director

SUBJECT: Draft Inspection Report No. OSE-14816, *Additional Senior Management Attention Needed to Strengthen USPTO's Information Security Program*

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

The USPTO is committed to developing a strong IT Security Program to protect the information assets of the USPTO and its customers, which are vital to the economic development and advancement of the country. I will continue to work with the USPTO Chief Information Officer (CIO), Doug Bourgeois, so that he and his staff can develop and implement an effective IT Security Program across the USPTO.

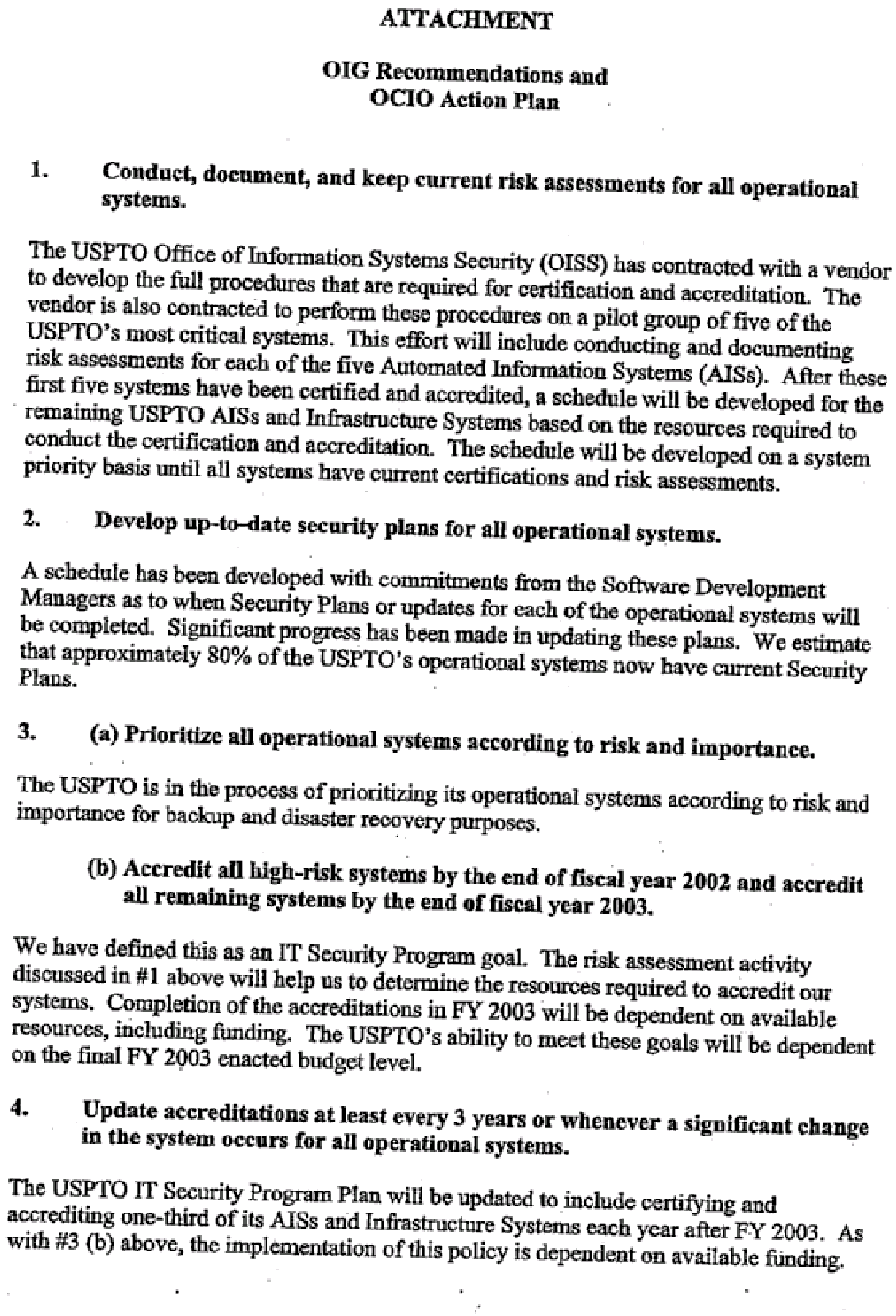
If you have any questions or wish to discuss any of the above items, please contact Susan Callis, IT Security Program Manager, at (703) 305-3898 or Susan.Callis@USPTO.gov.

Nicholas P. Godici
fr JAMES E. ROGAN

Attachment

cc: Nicholas P. Godici, Commissioner for Patents
Anne H. Chasser, Commissioner for Trademarks
Robert L. Stoll, Administrator for External Affairs
James A. Toupin, General Counsel
Clarence C. Crawford, Chief Financial Officer and Chief Administrative Officer
Sandra L. Weisman, Deputy Chief Financial Officer and Comptroller
Michelle Picard, Acting Director, Office of Finance

ATTACHMENT A



ATTACHMENT

OIG Recommendations and OCIO Action Plan

1. **Conduct, document, and keep current risk assessments for all operational systems.**

The USPTO Office of Information Systems Security (OISS) has contracted with a vendor to develop the full procedures that are required for certification and accreditation. The vendor is also contracted to perform these procedures on a pilot group of five of the USPTO's most critical systems. This effort will include conducting and documenting risk assessments for each of the five Automated Information Systems (AISs). After these first five systems have been certified and accredited, a schedule will be developed for the remaining USPTO AISs and Infrastructure Systems based on the resources required to conduct the certification and accreditation. The schedule will be developed on a system priority basis until all systems have current certifications and risk assessments.

2. **Develop up-to-date security plans for all operational systems.**

A schedule has been developed with commitments from the Software Development Managers as to when Security Plans or updates for each of the operational systems will be completed. Significant progress has been made in updating these plans. We estimate that approximately 80% of the USPTO's operational systems now have current Security Plans.

3. **(a) Prioritize all operational systems according to risk and importance.**

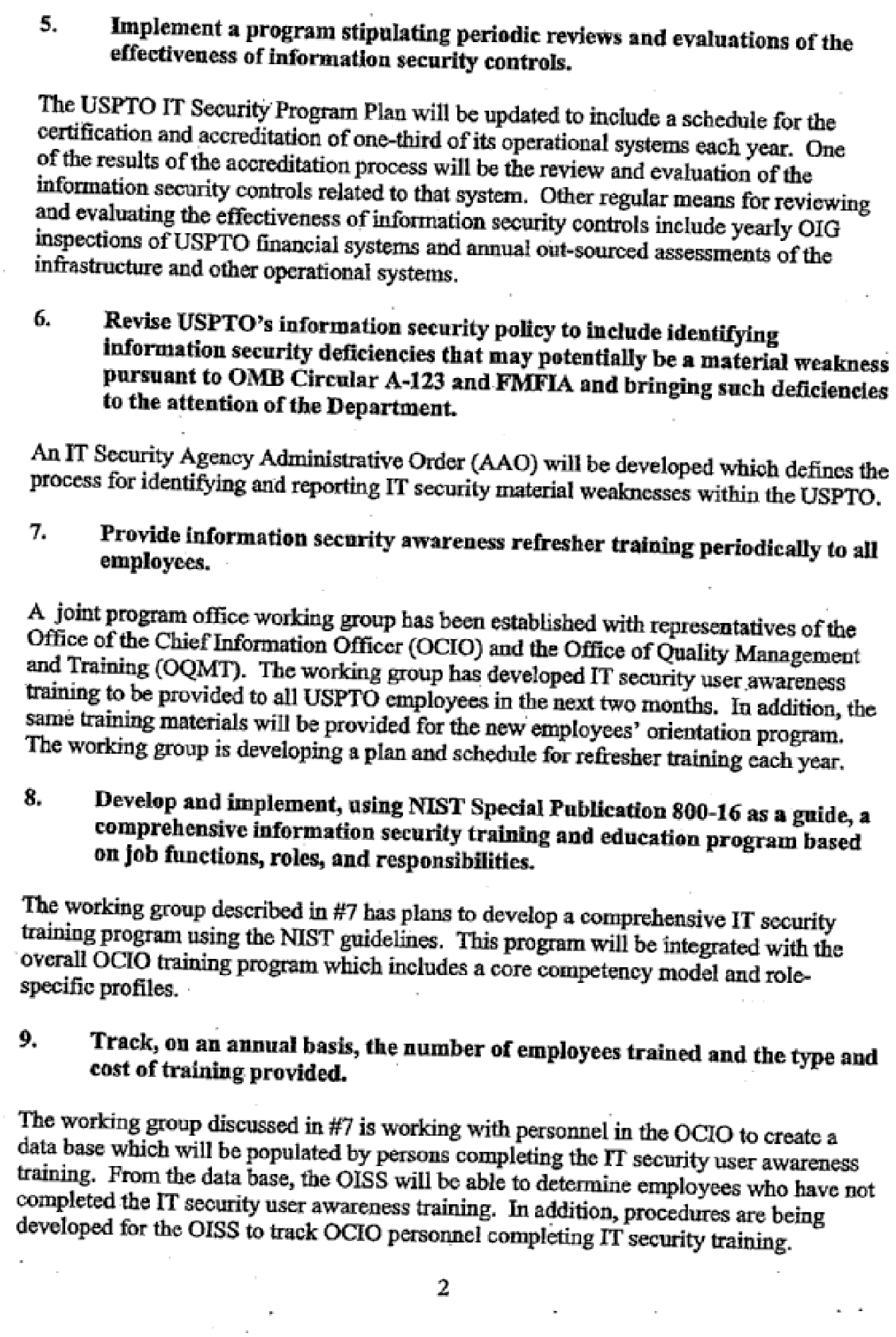
The USPTO is in the process of prioritizing its operational systems according to risk and importance for backup and disaster recovery purposes.

(b) Accredit all high-risk systems by the end of fiscal year 2002 and accredit all remaining systems by the end of fiscal year 2003.

We have defined this as an IT Security Program goal. The risk assessment activity discussed in #1 above will help us to determine the resources required to accredit our systems. Completion of the accreditations in FY 2003 will be dependent on available resources, including funding. The USPTO's ability to meet these goals will be dependent on the final FY 2003 enacted budget level.

4. **Update accreditations at least every 3 years or whenever a significant change in the system occurs for all operational systems.**

The USPTO IT Security Program Plan will be updated to include certifying and accrediting one-third of its AISs and Infrastructure Systems each year after FY 2003. As with #3 (b) above, the implementation of this policy is dependent on available funding.



5. **Implement a program stipulating periodic reviews and evaluations of the effectiveness of information security controls.**

The USPTO IT Security Program Plan will be updated to include a schedule for the certification and accreditation of one-third of its operational systems each year. One of the results of the accreditation process will be the review and evaluation of the information security controls related to that system. Other regular means for reviewing and evaluating the effectiveness of information security controls include yearly OIG inspections of USPTO financial systems and annual out-sourced assessments of the infrastructure and other operational systems.

6. **Revise USPTO's information security policy to include identifying information security deficiencies that may potentially be a material weakness pursuant to OMB Circular A-123 and FMFIA and bringing such deficiencies to the attention of the Department.**

An IT Security Agency Administrative Order (AAO) will be developed which defines the process for identifying and reporting IT security material weaknesses within the USPTO.

7. **Provide information security awareness refresher training periodically to all employees.**

A joint program office working group has been established with representatives of the Office of the Chief Information Officer (OCIO) and the Office of Quality Management and Training (OQMT). The working group has developed IT security user awareness training to be provided to all USPTO employees in the next two months. In addition, the same training materials will be provided for the new employees' orientation program. The working group is developing a plan and schedule for refresher training each year.

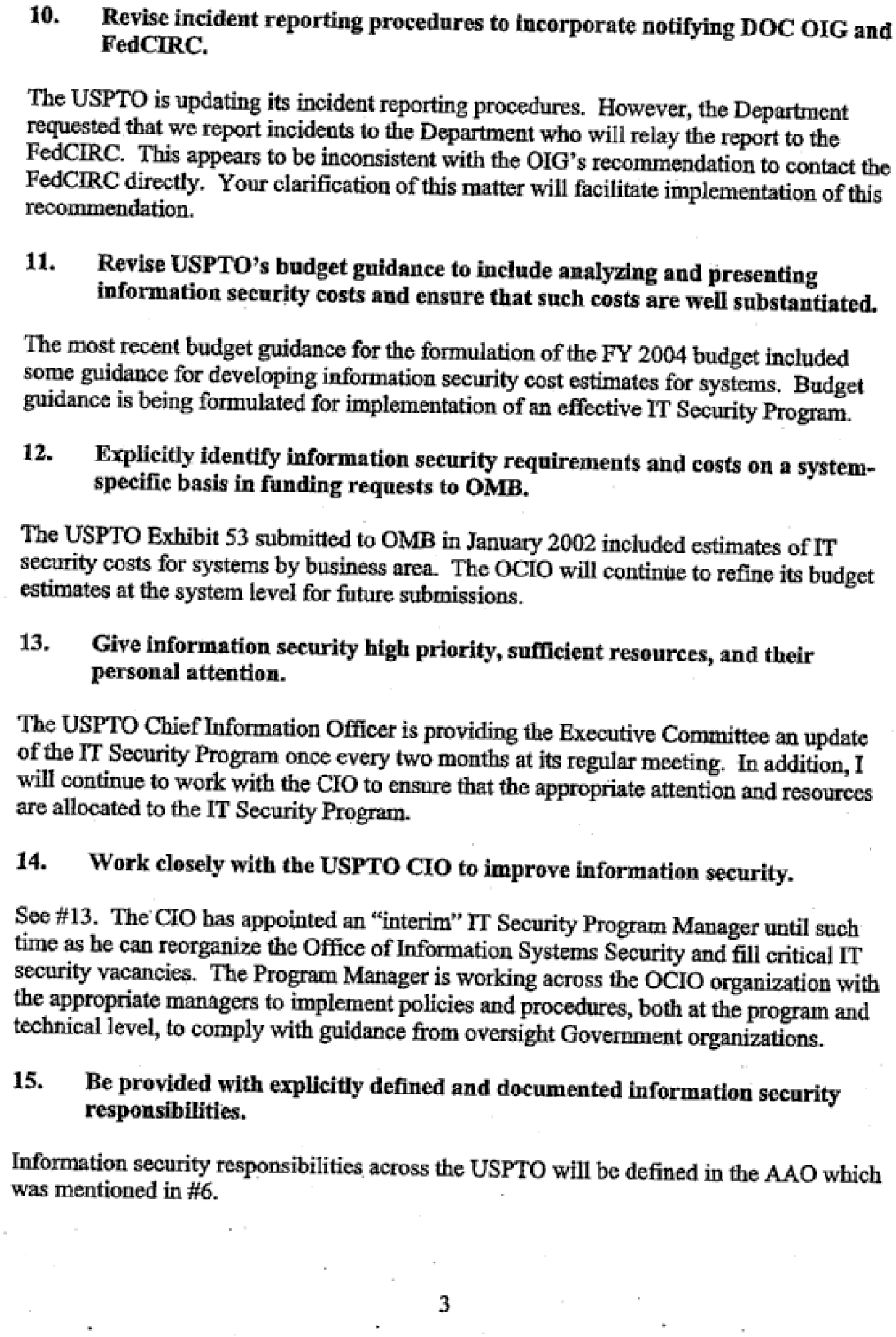
8. **Develop and implement, using NIST Special Publication 800-16 as a guide, a comprehensive information security training and education program based on job functions, roles, and responsibilities.**

The working group described in #7 has plans to develop a comprehensive IT security training program using the NIST guidelines. This program will be integrated with the overall OCIO training program which includes a core competency model and role-specific profiles.

9. **Track, on an annual basis, the number of employees trained and the type and cost of training provided.**

The working group discussed in #7 is working with personnel in the OCIO to create a data base which will be populated by persons completing the IT security user awareness training. From the data base, the OISS will be able to determine employees who have not completed the IT security user awareness training. In addition, procedures are being developed for the OISS to track OCIO personnel completing IT security training.

2



10. Revise incident reporting procedures to incorporate notifying DOC OIG and FedCIRC.

The USPTO is updating its incident reporting procedures. However, the Department requested that we report incidents to the Department who will relay the report to the FedCIRC. This appears to be inconsistent with the OIG's recommendation to contact the FedCIRC directly. Your clarification of this matter will facilitate implementation of this recommendation.

11. Revise USPTO's budget guidance to include analyzing and presenting information security costs and ensure that such costs are well substantiated.

The most recent budget guidance for the formulation of the FY 2004 budget included some guidance for developing information security cost estimates for systems. Budget guidance is being formulated for implementation of an effective IT Security Program.

12. Explicitly identify information security requirements and costs on a system-specific basis in funding requests to OMB.

The USPTO Exhibit 53 submitted to OMB in January 2002 included estimates of IT security costs for systems by business area. The OCIO will continue to refine its budget estimates at the system level for future submissions.

13. Give information security high priority, sufficient resources, and their personal attention.

The USPTO Chief Information Officer is providing the Executive Committee an update of the IT Security Program once every two months at its regular meeting. In addition, I will continue to work with the CIO to ensure that the appropriate attention and resources are allocated to the IT Security Program.

14. Work closely with the USPTO CIO to improve information security.

See #13. The CIO has appointed an "interim" IT Security Program Manager until such time as he can reorganize the Office of Information Systems Security and fill critical IT security vacancies. The Program Manager is working across the OCIO organization with the appropriate managers to implement policies and procedures, both at the program and technical level, to comply with guidance from oversight Government organizations.

15. Be provided with explicitly defined and documented information security responsibilities.

Information security responsibilities across the USPTO will be defined in the AAO which was mentioned in #6.