U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

UNITED STATES PATENT AND TRADEMARK OFFICE

Independent Evaluation of USPTO's Information Security Program Under the Government Information Security Reform Act

Executive Summary

Final Inspection Report No. OSE-15250/September 2002

PUBLIC RELEASE

Office of Systems Evaluation

TABLE OF CONTENTS

INTRODUCTION

The Government Information Security Reform Act (GISRA), Title X, subtitle G, of the 2001 Defense Authorization Act (P.L. 106-398) was signed into law on October 30, 2000. This law contains a subchapter that primarily addresses managing, implementing, overseeing, and ensuring the security of unclassified and national security information systems.

GISRA requires (1) annual agency program reviews; (2) annual independent OIG evaluations; (3) agency reporting of the results of OIG evaluations to the Office of Management and Budget (OMB); and (4) an annual OMB report to Congress summarizing the agency materials received.

In accordance with OMB guidance, agency heads are to transmit to OMB both OIG's independent evaluation and the agency's program review along with fiscal year budget materials. As a performance-based organization, the United States Patent and Trademark Office (USPTO) submits its budget materials and information security review separate from those of the Department of Commerce. For FY01, we submitted the same independent evaluation for USPTO as for the Department because our evaluation addressed the status and issues associated with the Department as a whole, including USPTO. However, because USPTO is undertaking actions separate from the Department's to manage information security, we have reviewed USPTO's information security program separately in FY02. This report summarizes the results of that separate review.

USPTO's Fiscal Year 2001 GISRA Reporting

In conducting its own FY01 GISRA review, USPTO used NIST's *Security Self-Assessment Guide for Information Technology Systems*,[1] as recommended by OMB. This guide establishes five levels of program effectiveness—level 5 being the highest (see Figure 1)—and identifies steps that must be taken to achieve each assessment level.

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 1. Levels of Information Security Effectiveness

Based on its self-assessment, USPTO reported for FY01 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, stating, "With current funding levels, USPTO will meet 75 percent of level 5

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

compliance of GISRA at the end of FY 2002. However, we expect to achieve 100 percent compliance by the end of FY 2003."

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 here, confirm this rating. In FY02, USPTO reassessed its status and told us that, consistent with our evaluation, it now considers itself at level 2.

OBJECTIVES, SCOPE, AND METHODOLOGY

We sought to determine whether USPTO's information security program and practices comply with the requirements of GISRA, which mandates that federal agencies have effective security measures for the information resources that support their operations. Our evaluation for FY02 is based on the results of the following OIG reviews and audits:

- *Additional Senior Management Attention Needed to Strengthen USPTO's Information Security Program,* Final Inspection Report No. OSE-14816/March 2002. Evaluation of organization-wide information security policies and procedures, staff roles and responsibilities, and the program's compliance with applicable laws, regulations, and guidance.

- *Stronger Management Controls Needed for the Patent Application Capture and Review Automated Information System,* Inspection Report No. OSE-14926/August 2002. Evaluation of information security controls for the Patent Application Capture And Review (PACR) system, which 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.

- *Improvements Needed in the General Controls Associated with USPTO's Financial Management Systems,* Audit Report No. FSD-14477-2-0001/February 2002. Audit of general controls associated with the IT processing environment conducted as part of OIG's FY01 financial statements audit. This report included a follow-up review of the general controls associated with the Revenue Accounting and Management System and the Federal Financial System (U.S. Geological Survey's standardized financial system that provides financial services to USPTO), and an examination of the controls over USPTO's public key infrastructure environment.[2]

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

- *Network Vulnerability Assessment Improvements Needed in the General Controls Associated with USPTO's Financial Management Systems,* Audit Report No. FSD-14477-2-0003/March 2002. Also part of OIG's FY01 financial statements audit, this review was a limited network vulnerability assessment of USPTO's local area network, PTONet.

We conducted our evaluation using the following criteria: NIST's *Security Self-Assessment Guide for Information Technology Systems*, GISRA, the Computer Security Act, and OMB Circular No. A-130, "Management of Federal Information." An OIG contractor conducted the general control reviews of financial systems and related networks, using GAO's *Federal Information System Controls Audit Manual* as a guide.

The structure and content of this report respond to guidance provided by OMB in *Reporting on the Government Information Security Reform Act.* The report is being issued in final because it is based primarily on prior OIG work that has been presented in previous reports and because it makes no new recommendations. We do not address critical infrastructure issues because USPTO has no assets considered critical under the critical infrastructure protection program.

We performed our work in accordance with the Inspector General Act of 1978, as amended, and the *Quality Standards for Inspections*, March 1993, issued by the President's Council on Integrity and Efficiency.

FINDINGS

I. USPTO Should Report Information Security as a Material Weakness

GISRA requires that significant deficiencies in security policy, procedures, or practices be reported as material weaknesses. OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," instructs agencies to identify security deficiencies pursuant to OMB Circular A-123, "Management Accountability and Control," if it is determined that there is no assignment of security responsibility, no security plan, or no accreditation. The agency's decision to report a material weakness should depend on the risk and magnitude of harm posed by the weakness. Failure to report significant information security weaknesses could result in the failure to mitigate unacceptably high security risks.

As discussed in this report, our evaluation found that USPTO lacks up-to-date security plans and current accreditations for its operational systems; in our opinion, USPTO should consider information security a material weakness. We recommended that USPTO determine whether this area is a potential material weakness to be brought to the attention of the Department, which would then determine whether it is significant enough to report to the President and Congress. Additionally, we recommended that USPTO revise its information security policy to identify information security deficiencies that are material weaknesses pursuant to OMB Circular A-123 and the Federal Managers' Financial Integrity Act (FMFIA), and bring them to the Department's attention.

USPTO has agreed to revise its information security policy and will develop an administrative order that defines the process for identifying and reporting material weaknesses to the Department. USPTO officials told us that in reporting to the Department under OMB Circular A-123 and FMFIA for FY02, they are seriously considering identifying information security as a material weakness, but have made no decision yet. Until all of USPTO's mission-critical systems are accredited, we believe that information security should be reported as a material weakness.

II. USPTO's Top Leadership Has Made a Commitment to Improving Information Security

A. Long-standing Information Security Weaknesses Require Senior Management Attention

To safeguard the privacy, confidentiality, and security of federal information, GISRA makes the head of an agency responsible for ensuring that security plans for the agency's information systems are in force throughout each system's life cycle and promoting security as an integral component of that agency's business operations. Our evaluation found that, until recently, information security had not received adequate attention at USPTO. As a result, significant weaknesses exist in planning, budgeting, implementing, reviewing, and overseeing this area.

Specifically, we found a lack of follow-through in carrying out fundamental responsibilities, including

- identifying, assessing, and understanding risks to IT assets;
- determining security needs commensurate with 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 information security policy and the effectiveness of related practices; and
- integrating security into capital planning and investment control processes.

Since the time of our evaluation, the Under Secretary of Commerce for Intellectual Property and Director of USPTO has made a commitment to protect the bureau's information assets and is devoting additional attention and resources to this area.

B. The Director Is Taking Action to Support Information Security Improvements

In our report, *Additional Senior Management Attention Needed to Strengthen USPTO's Information Security Program,* we noted that the awareness, support, and proactive involvement of USPTO's senior management are essential to establishing the environment and ensuring the resources needed to promote an effective information security program. We recommended that the USPTO Director ensure that senior management officials give information security high priority, sufficient resources, and their personal attention; work closely with the USPTO chief information officer (CIO) to improve information security; and be provided with explicitly defined and documented information security responsibilities.

The Director agreed with these recommendations. According to the corrective action plan USPTO submitted in response to the above-cited OIG report, the CIO regularly briefs the Director and the Executive Committee on the status of efforts to strengthen information security. Because this committee deals with all budget issues and reviews the strategic information technology plan, no significant IT investment can be made without its concurrence. Therefore, USPTO has a structure in place to ensure that information security is planned for all significant IT investments and receives appropriate attention throughout an investment's life cycle.

Additionally, the Director has authorized the CIO to add six information security staff positions, has reallocated FY02 funding for information security program improvements, and is seeking increases in base spending for information security. The Director has also approved several initiatives to revise information security operations and controls (see page 13) and to provide a

framework for improving overall compliance with the requirements for management and operational controls.

USPTO's new strategy, presented in *The 21st Century Strategic Plan,*[3] further demonstrates the Director's commitment to improving information security. Referring to the OIG reports on which our independent evaluation is based, the plan states that USPTO is not in compliance with the law and that because information security has not yet become an integral part of USPTO's business operations, fundamental IT security responsibilities are frequently not carried out. The plan concludes that the implication of not being compliant with GISRA is that neither internal nor external customers can trust USPTO's automated information systems and presents tasks, milestones, and a schedule for correcting this problem that are consistent with our recommendations. It also proposes using data replication for disaster recovery, an important element of information security.

III. Incident Response Reporting and Handling Procedures Are Being Revised

OMB Circular A-130 requires agencies to establish formal incident response mechanisms for 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. GISRA expands on this 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) when such an incident occurs.

We found that USPTO's documentation of response procedures for information security incidents is consistent with OMB Circular A-130. Its documents appropriately identify roles and responsibilities, define incident types and severity levels, and have reporting requirements. However, USPTO does not require that OIG and external security offices and authorities be notified or consulted. For the period from October 2000 to October 2001, USPTO recorded several high-severity information security incidents, but did not report any to FedCIRC or OIG.

We recommended that USPTO revise its incident handling procedures to include the reporting of such events to both FedCIRC and OIG. USPTO agreed and will implement this recommendation by reporting incidents to the Department, which will then relay the information to FedCIRC and OIG, as appropriate.

IV. USPTO Program Officials and CIO Need to Ensure That Management Controls Are Fully Implemented

GISRA requires agency managers and program officials to ensure that effective information security policies and procedures are implemented throughout the life cycle of every IT system. The agency CIO is required to assist other senior officials with their information security responsibilities, as well as ensure that effective policies and procedures are implemented for the systems that support the CIO's functions. Our evaluation found that program officials have not

[3]U.S. Patent and Trademark Office, June 3, 2002. *The 21st Century Strategic Plan.* Washington, DC: USPTO.

given sufficient attention to the security of the information assets that support their operations. The first two sections of this finding discuss the observations and recommendations we made as a result of our fieldwork; the third section addresses the steps that USPTO has taken or planned in response.

A. Risk Assessments Have Not Been Completed, Security Plans Are Outdated, and Controls Have Not Been Tested

Program officials are responsible for information security management controls—assessing the risks to the operations and assets over which they have authority, determining the level of information security to protect such operations and assets, and periodically testing and evaluating information security controls and techniques. As shown in Figure 2, at the time of our evaluation, 64 of USPTO's 78 operational systems[4] (or 82 percent) lacked documented risk assessments, and the security plans for 24 of those systems (30 percent) were more than 3 years old. Systems supporting the missions of program officials and the CIO lacked up-to-date risk assessments and security plans. We recommended that USPTO conduct, document, and keep current, risk assessments for all operational systems; develop up-to-date security plans for these systems; and implement a program stipulating periodic reviews and evaluations of the effectiveness of information security controls.

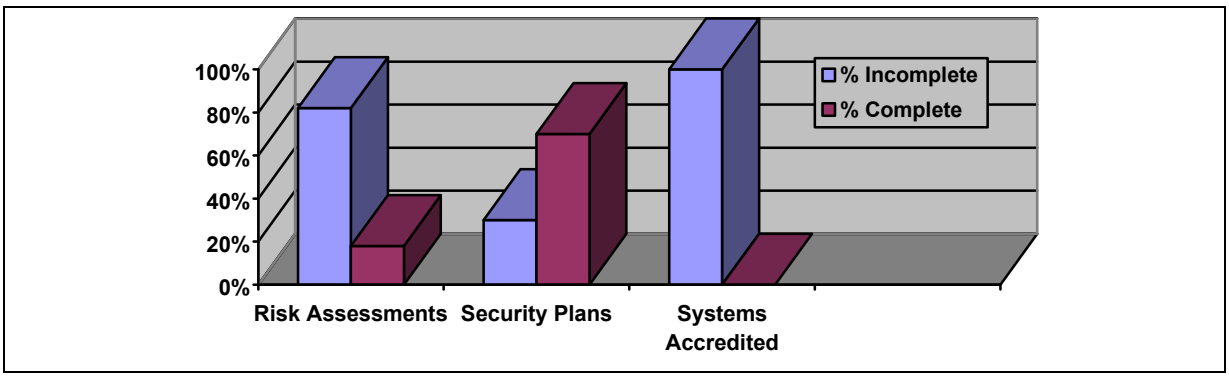

Figure 2. Status of USPTO's Key Information Security Management Controls at Time of OIG Evaluation (December 2001)

B. 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 responsibility for the risks associated with putting the system into operation. The authorization is based on an assessment of the system's management,

[4] Since the time of our evaluation, USPTO has revised its system inventory.

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 reauthorized following any significant change or at least every three years, and more often where risk and potential magnitude of harm are high.

At USPTO, accreditation is a shared 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.

We found that none of USPTO's operational systems has a current authorization to process (accreditation), and until recently, little attention was given to accreditation. 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 recommended that USPTO prioritize all operational systems according to risk and importance, 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 also recommended that accreditations be updated at least every three years or whenever a significant change in a system occurs.

C. USPTO Is Taking Steps to Strengthen Management Controls

USPTO responded to our recommendations by providing funding and developing approaches to address the problems we identified. Specifically, the CIO has initiated a pilot project to establish a certification and accreditation process for five information systems. As part of the process, risk assessments, security plans, and contingency plans are being prepared, and security tests and evaluations performed. The pilot will validate staffing and cost estimates for USPTO's information security program budget request. After the pilot is completed, the process will be extended to USPTO's other information systems.

USPTO preliminarily ranked its systems by risk and criticality, but concluded that it cannot achieve the accreditation schedule we had recommended. Instead, it plans to accredit all high-risk systems by the end of FY03 and the remaining systems by the end of FY04. Because of the large amount of work USPTO has to perform to complete the accreditations and the importance of employing a meaningful and effective accreditation process, we agreed with this timetable. USPTO does, however, intend to have up-to-date security plans for all of its systems by the end of FY02 and to update them on a 3-year cycle as part of certification and accreditation.

V. Improvements Are Needed in USPTO-Wide Security Program Implementation, Life Cycle Management, Training, and Capital Investment Planning

GISRA requires agency CIOs to administer the information security program agencywide, a process that entails developing the security program, ensuring it is effectively implemented and maintained, and training and overseeing personnel who have significant responsibilities for information security. Our evaluation found that USPTO needs improvements in all of these areas. The first four sections of this finding discuss the observations and recommendations we made as a result of our fieldwork; the fifth section addresses the steps that USPTO has taken or planned in response.

A. Policies and Procedures Exist but Often Are Not Implemented

We found that USPTO generally has documented policies and procedures in place that are consistent with accepted security practices. However, as the foregoing discussions show, often these policies and procedures are not implemented. Moreover, the CIO needs to work with other senior agency officials to periodically evaluate the effectiveness of USPTO's information security program, including testing control techniques.

B. Life Cycle Management Deficiencies Should Be Corrected

Security Effects of Network Upgrade Were Not Well Planned

During our evaluation of PACR, USPTO was transitioning from its local area network (LAN), PTONet, to the more capable and technologically current PTONet II. Because USPTO's LAN supports patent application processing, the transition required changes to PACR network components and related software.

However, these changes were not well planned and did not adequately consider network security implications. Just prior to the initial transition step for PACR, USPTO was unable to identify required software changes and necessary modifications to firewall rules. Furthermore, the information system security officer was unaware that these changes were about to be made, even though he was also the acting director of the Office of Information Systems Security, which is responsible for reviewing and authorizing proposed firewall changes.

USPTO issued draft procedures for implementing PACR network and firewall changes after initial transition attempts failed. Since the conclusion of our fieldwork, USPTO successfully completed the transition of PACR to PTONet II. USPTO needs to better plan and coordinate IT changes that affect the security of interconnected systems.

Documentation Was Inaccurate

System documentation should be current and accurate to support testing, training, modification, and maintenance. The quality and utility of supporting documentation is a primary measure of the health and well-being of a software project.[5]

In our review of PACR, we found that although security plans had been developed, USPTO was unable to provide official sign-off pages or documented Technical Review Board[6] action to indicate that any of these plans had been officially approved. Moreover, in examining the available system documentation for our PACR review and attending briefings provided by USPTO, we found that

- the documentation did not reflect the current system;
- network topology diagrams, four in all, had the same issue date but each differed from the others and none accurately described the then-current or planned topology; and
- discrepancies existed between the network topology diagrams, equipment lists, and points of contact specified in the High-level Architecture document and Operational Support Plan.

In looking at USPTO's management system for IT documentation, we found problems with security documentation for other systems as well. We recommended that documentation be updated to reflect the current operational system, and a process to track document approval be established and enforced.

C. Information Security Awareness, Training, and Education Need Improvement

USPTO's information security awareness program covers the areas identified by OMB Circular A-130 and other applicable guidance; at the time of our fieldwork however, awareness training was 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 guidance states that a stimulus used repeatedly will eventually be selectively ignored. Therefore, we recommended that USPTO provide periodic refresher training to all employees to assure that they continue to understand and abide by the applicable rules.

In addition, USPTO does not have an adequate training and education program for personnel who need specialized security skills and competencies. Information security officers and other employees who have security responsibilities receive some relevant training, but that training is not sufficient, and USPTO lacks a formal program for giving employees security training

[5] Fairley, R. 1985. *Software Engineering Concepts*. New York: McGraw-Hill, p. 220.
[6] The Technical Review Board conducts reviews of work products and plans during the life cycle of an information system. The board is chaired by the deputy CIO and attended by the systems development manager for the project from the CIO's office and the project manager from the project sponsor's business unit.

applicable to their job function. Without such a program, USPTO cannot ensure that employees who have security responsibilities, including its security professionals, understand and apply information security practices effectively. We recommended that USPTO establish a formal training program that gives all personnel who have significant security responsibilities an understanding of those responsibilities and of information security risks.

D. 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. OMB Circular A-11, which governs preparing and submitting budget estimates, stipulates that security costs be presented in Exhibit 53, "Agency IT Investment Portfolio," as a percentage of the total system cost or project investment and that capital asset plans be provided in Exhibit 300, "Capital Asset Plan and Business Case," indicating whether the project's security meets GISRA requirements and describing the security and privacy measures to be used.

However, USPTO did not identify security costs for any individual system in its FY02 or FY03 budget submissions. Even if a security funding request had been included, the amount would have been questionable because USPTO had not conducted an accurate, thorough analysis of current security needs or of the cost of satisfying them. Furthermore, FY02-FY07 budget formulation guidance provided by USPTO's Office of the Chief Information Officer did 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 cannot justify funding needed to plan and implement required security improvements. We recommended that USPTO explicitly identify information security requirements and costs on a system-specific basis in funding requests to OMB

E. USPTO Is Taking Action to Improve Security Program Implementation, Life Cycle Management, Training, and Capital Investment Planning

In addition to strengthening management controls (see Finding IV), the CIO is working to improve overall information security operations by restructuring the Office of Information System Security and enhancing other areas we identified as problematic: (1) policies that govern information security practices, (2) programs for training employees and contractors, and (3) processes for budgeting and planning for IT capital assets.

Office of Information System Security Restructuring. The CIO is separating policy and compliance functions from security operations—a move that should increase the office's effectiveness—and is adding six new staff positions. Pending adequate staffing, the office has been headed by an acting IT security program manager who reports directly to the CIO and is responsible for managing USPTO's information security improvement efforts. To remain in

compliance with GISRA, this senior information security official should report to the CIO on a permanent basis.

Policies. In order to provide the basic foundation for information security, the CIO is preparing an administrative order that will describe USPTO's information security policies and clarify staff roles and responsibilities. The CIO has also begun working with information security program managers to develop procedures for periodically evaluating the effectiveness of information security controls. Procedures for controlling security documentation are to be revised by the end of the calendar year.

Training. All USPTO employees and contractors completed security awareness training as of June 30, 2002. A working group is developing a plan for providing information security training that is specific to the individual responsibilities of all USPTO employees, with training for managers and technical personnel to begin in late September 2002. A database has been established to track employee training.

Budgeting and Planning. An information security budget has been developed that allocates funding for many needed improvements including

- certification and accreditation,
- self-assessments using the NIST *Self-Assessment Guide*,
- compliance testing of a sample of information systems,
- design and implementation of a host-based intrusion detection system,
- contractor support for correction of information system vulnerabilities, and
- information security training for users, managers, and technical personnel.

The Office of the CIO's budget system has been enhanced so that information security costs can be budgeted and tracked for each system, and funding for information security has been included in each system's budget plan.

VI. Information Security Requirements Need to Be Included in USPTO's Information Technology Service Contracts

As outsourcing of IT services increases, the risk of security violations by contractors—whether inadvertent or deliberate—also grows. In last year's GISRA report, we identified problems with information security in IT service contracts, most notably, a lack of sufficient policy and guidance to ensure that contract documents for IT services contain adequate information security provisions. In FY02, we examined this weakness in greater detail: we reviewed 40 of the Department's IT service contracts, including some awarded by USPTO, and found that provisions to safeguard sensitive but unclassified systems and information were either insufficient or nonexistent. Based on the results of this sample, it is likely that the majority of IT service contracts throughout the Department lack needed information security provisions. Contracting officers and other acquisition team members need sufficient guidance and training, as well as support from technical experts and program officials, to ensure that they prepare and administer IT service contracts in a way that makes clear and enforceable the contractor's responsibility and accountability for safeguarding the government's information assets.

We recommended that the Department of Commerce's Chief Financial Officer and Assistant Secretary for Administration take the necessary actions to ensure that all contracting offices within Commerce, including USPTO, include adequate information security provisions in all IT service contracts in order to protect the Department's sensitive IT information and assets. Specifically, we urged the Department to establish standard contract provisions for safeguarding the security of unclassified systems and to disseminate clear, detailed policy for acquiring these systems and services.

We further recommended that such policy require contracting offices—with assistance from the Department's Office of the CIO—to assess the information security risk associated with the proposed service or system during the acquisition planning phases; identify and include appropriate information security requirements in specifications and work statements; monitor contractor performance to ensure compliance with information security requirements; and terminate the contractor's access to systems and networks once the contract is closed out. We also advised the Department to review all current contracts and solicitations for IT services to determine whether information security provisions should be added to them, even though such revisions may increase contract costs, and to ensure that all procurement personnel have appropriate training in information security. The CFO agreed with our recommendations and is taking actions to implement them.

Officials in USPTO's Office of Procurement told us that they generally agree with the findings and recommendations contained in our report pertaining to ensuring that adequate information security provisions are included in all IT service contracts and providing appropriate training in information security. They indicated, however, that due to USPTO's unique status, it may not be subject to some of the specific documents and policies identified in the report and intend to get input from the Office of the CIO. The Offices of Procurement and CIO need to work together, along with program officials, to ensure that adequate information security requirements are included and followed in all of USPTO's IT service contracts.

VII. USPTO's Corrective Action Plan Establishes a Solid Foundation for Improving Information Security

In FY02, USPTO completely reworked its GISRA corrective action plan so that it lays out a cohesive roadmap for improving information security. USPTO's plan is organized by the three control areas—management, operational, and technical—identified in NIST's *Security Self-Assessment Guide.* The plan goes beyond the recommendations in our reports to identify additional actions needed in each control area for achieving a comprehensive information security program. Actions are added to the plan as new requirements are identified.

While USPTO has completed or is expecting to meet the schedule for about 80 percent of the milestones in its action plan, some important milestones are slipping. These include developing the administrative order on information security policies, completing the certification and accreditation pilot project, developing system-level procedures, and preparing a disaster recovery plan for USPTO's infrastructure.

We believe, however, that USPTO is making a determined effort to improve its information security program and meet its milestones. Some of the delay is attributable to USPTO's attempt to instill information security processes that will yield quality products and provide the needed degree of assurance. We anticipate that USPTO's rate of progress will increase as it hires a permanent IT security manager, fills its new information security positions, and continues to give senior management attention to this area.