U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

PUBLIC RELEASE

OFFICE OF THE SECRETARY

Independent Evaluation of the Department of Commerce's Information Security Program Under the Federal Information Security Management Act

Final Inspection Report No. OSE-16146/September 2003

Office of Systems Evaluation

CONTENTS

EXECUTIVE SUMMARY

The Federal Information Security Management Act (FISMA), signed into law on December 17, 2002, provides a comprehensive framework for ensuring that information resources supporting federal operations and assets employ effective security controls. FISMA requires agencies to conduct annual information security program reviews and Offices of Inspector General (OIGs) to perform annual independent evaluations of those programs. Our independent evaluation for FY 2003 sought to determine whether the Department of Commerce's information security program and practices for unclassified systems comply with FISMA.

As a performance-based organization, the United States Patent and Trademark Office (USPTO) has submitted its budget materials, information security review, and *Performance and Accountability Report* separate from those of the Department. For the past 2 fiscal years, we prepared a separate independent evaluation report on USPTO. For fiscal year 2003, however, we have included USPTO in this single, Commerce-wide evaluation report, as has the Department in its OMB submission. This consolidation is in keeping with OMB's FY 2002 Report to Congress on federal government information security reform, in which it combined USPTO with the rest of Commerce.

The structure and content of this report are designed to be responsive to the guidance provided by OMB in *Reporting Instructions for the Federal Information Security Management Act,* while also providing useful information for Commerce officials. As directed in this guidance instructions, we begin with our response to question A.2.a.

Total number of programs, systems, and contractor operations or facilities evaluated in FY 2003. (OMB Question A.2.a)

Our evaluation is based on the results of OIG reviews and audits of 43 systems in 9 of Commerce's 14 operating units. These assessments looked at (1) selected systems at the National Oceanic and Atmospheric Administration (NOAA); (2) general controls of financial systems (reviewed as part of the FY 2002 consolidated financial statement audit and financial statement audits of the National Technical Information Service (NTIS) and USPTO); (3) status of the issues identified at the National Institute of Standards and Technology (NIST) and USPTO in our in-depth evaluation of these organizations last year; and (4) risk assessments, security plans, contingency plans, security test and evaluation materials (test procedures and results), certification and accreditation[1] documents, capital asset plans (Exhibit 300s), and plans of action and milestones (POA&Ms)[2] for a range of operating unit systems. We obtained additional information through interviews with the chief information officers (CIOs) and senior information security officials of the Department, Census Bureau, International Trade Administration (ITA), NIST, NOAA, and USPTO.

[1] Certification is the formal testing and evaluation of the security safeguards on 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.
[2] OMB guidance directs agencies to develop plans of action and milestones (POA&Ms) to correct program- and system-level IT security weaknesses and track each deficiency until it is corrected.

We also reviewed a random sample of 24 contracts awarded by Census, NIST, NOAA, Office of the Secretary, and USPTO for the period October 2002 through August 20, 2003, to assess the Department's progress in incorporating information security requirements into information technology (IT) service contracts. Our principal findings are summarized below.

Information security in IT service contracts. (OMB Question A.2 b-e)

Information Security in IT Service Contracts Is Improving, but Additional Efforts Are Needed. Commerce's IT expenditures accounted for nearly half ($500 million) of all contract obligations in FY 2002; some two-thirds of that amount (approximately $334 million) was for IT services. Our FY 2002 independent evaluation included a review of information security provisions in departmental contracts[3] for these services and found that most contracts had either insufficient security provisions or none at all. We concluded that federal and departmental policy and guidance for incorporating such provisions were lacking. In the intervening year, the Department issued its information security policy and drafted a standard contract provision—currently under departmental review—for safeguarding the security of unclassified systems and information. The draft provision requires, among other things, a system security plan and certification and accreditation for contracted IT resources/ services that involve connection to Commerce networks or storage of Commerce data on contractor-owned systems.

Our FY 2003 independent evaluation found that some progress has been made in incorporating security provisions into recent IT service contracts. However, there remains (1) a general absence of provisions for controlling access to Department systems and networks; and (2) little evidence of contract oversight, or of coordination among contracting, technical, and information security personnel in developing appropriate contract security requirements. We believe the general absence of such provisions and the inadequate interface among all staff involved in the contracting/information security process continue to place Commerce systems and data at risk. (See page 4.)

Agency's work to develop an inventory of major IT systems. (OMB Question A.2.f)

The Department Is Continuing to Refine its Systems Inventory. Commerce's new information security policy, issued in January 2003, requires all operating units to maintain a comprehensive systems inventory. Each unit, including USPTO, provides an updated copy of its inventory to the Department's IT security program manager twice a year. As part of its compliance reviews of information security, the Department's CIO Office is validating the inventory data, with emphasis on determining whether operating units are properly applying NIST criteria in defining system boundaries. (See page 6.)

Material weaknesses. (OMB Question A.3)

The Department Should Continue to Report Information Security as a Material Weakness. For the past 2 fiscal years, the Department has reported information security as a material weakness in its Accountability Report. In our FY 2002 independent evaluation, we stated that the Department should continue to report information security as a material weakness until all

[3] The term "contract" includes task orders and delivery orders issued under multiple award contracts and government-wide agency contracts (GWACs).

systems that are national critical (part of the critical infrastructure) and mission critical have been certified and accredited. The Department set a goal for certifying and accrediting these systems by the end of FY 2003. In our evaluation this year, we found numerous systems that have been reported as certified and accredited with significant deficiencies in their certification and accreditation materials—risk assessments, security plans, and contingency plans—and in most cases, lack evidence that security controls had been tested. These problems call into question the effectiveness of the certification and accreditation processes being used.

We understand that some of the certifications and accreditations that we reviewed are being reworked to meet the requirements of the Department's new information security policy.[4] However, given the shortcomings in the systems we evaluated, we do not believe that certification and accreditation of the Department's roughly 340 national-critical and mission-critical systems[5]—of sufficient quality and content—can be completed by the end of the fiscal year. Thus, while the Department is to be commended for its push to certify and accredit its critical systems, we believe that information security should be reported as a material weakness for FY 2003. We have worked closely with the Department CIO on information security concerns throughout the year, and he has indicated agreement with our conclusion. (See page 7.)

USPTO. Last year we found that USPTO lacked current certifications and accreditations for its systems and suggested that it report information security as a material weakness until its mission-critical systems are certified and accredited. (USPTO has no systems designated as national critical). USPTO reported information security as a material weakness in its FY 2002 Accountability Report, and set a goal of certifying and accrediting all high-risk systems by the end of FY 2003. The agency subsequently revised its systems inventory by consolidating more than 100 systems into 19 systems, 9 mission critical and the remainder business essential. It planned to have its 9 mission-critical systems and 1 classified system certified and accredited by the end of FY 2003. As of mid-September, all 10 systems had undergone certification testing, 5 had been granted interim accreditations, and 1 had received final accreditation. USPTO expects to grant the remaining 4 systems 120-day interim accreditations by the end of the fiscal year.

USPTO is employing a disciplined certification and accreditation process that includes rigorous testing of security controls. Interim accreditations are not granted without comprehensive risk assessments, security plans, and testing. But because of the security weaknesses being identified by the certification process and the lack of final accreditations, we believe that USPTO should report information security as a material weakness for FY 2003. (See page 8.)

Agencywide plan of action and milestone process. (OMB Question A.4)

The Department Has Established a Sound Plan of Action and Milestone (POA&M) Process. The requirements for POA&Ms are specified in the Department's information security policy and are responsive to the criteria in OMB's FY 2003 FISMA guidance. Commerce develops, implements, and manages POA&Ms for all of its systems that have identified security weaknesses. System owners[6] are required to prepare the POA&Ms for

[4] We obtained certification and accreditation materials from the operating units in June and July 2003.
[5] The number of systems is based on the Department's March 2003 system inventory.
[6] The Department's information security policy defines a system owner as a project manager with day-to-day

their systems, and the operating unit IT security officer prepares the POA&M for the unit's program. Operating units are required to submit their POA&Ms, including the status of corrective actions, to the Department CIO Office monthly. Commerce monitors POA&Ms closely and uses them to manage corrective actions for all identified weaknesses. OIG has access to all POA&Ms, but because many are based primarily on self-assessments, which may not identify all weaknesses, we place greater reliance for identifying weaknesses on independent reviews. Commerce's POA&M database does not include the accounting codes associated with each line of the IT budget request, and IT system and budget reviews do not formally take into account the content of the POA&Ms, although attention is given to information security in these reviews. The CIO Office intends to tie POA&Ms to the system budget request in FY 2004. (See page 9.)

USPTO. Like the Department, USPTO develops, implements, and manages POA&Ms for all of its systems that have identified security weaknesses. Its CIO Office develops the POA&Ms, collaborating with program officials to ensure that information security weaknesses are addressed. To satisfy OMB's guidance, program officials at USPTO need to have primary responsibility for the POA&Ms that support their operations. Beginning in FY 2004, USPTO will submit its POA&Ms to the Department's CIO Office for incorporation into Commerce's consolidated report to OMB. (See page 9.)

Steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials, and actions to implement and enforce these steps. (OMB Question B.1)

Responsibilities and Authorities Are Clearly Specified for the Department CIO and Operating Unit Officials. The responsibilities and authorities for the Department's CIO and program officials have been clearly specified in the new information security policy. Accordingly, the CIO has primary oversight of all aspects of Commerce's information security program and reports to the Deputy Secretary on the status of information security within the Department. Operating unit heads have explicit responsibility for the unit's information security, and program officials—members of an operating unit's top-level management team—must ensure the implementation of an effective information security program for the systems under their responsibility.

In July 2001, the Secretary directed secretarial officers and heads of operating units to give information security high priority and sufficient resources. Over the past 2 years, the Deputy Secretary has reinforced this direction and given the Department CIO strong support for improving information security. Indeed, we believe that the progress made by Commerce in information security is attributable not only to the formal authority granted to the CIO position and the vigorous efforts of that official, but also to the Deputy Secretary's support, which has significantly enhanced the CIO's effectiveness. Simply stated, operating unit heads understand that information security is a priority for the Deputy Secretary and that they need to be responsive to issues raised by the Department CIO.

In addition, corrective actions at NIST demonstrate that operating unit heads are better recognizing their new responsibilities. Last year we performed an in-depth review of NIST's

---

management and operational control over the system and direct oversight of the system/network administrators and operations staff.

information security program, which identified numerous weaknesses. In response to our findings, the NIST director took significant improvement actions. This year, we found that NIST has made excellent progress in responding to our concerns and improving its information security program. (See page 12.)

USPTO. The information security responsibilities and authorities for the agency's CIO and program officials are delineated in USPTO's draft Agency Administrative Order (AAO) 212-4, *Information Technology Security*, which is expected to be finalized by the end of the fiscal year. Our independent evaluation last year reported that USPTO had long-standing information security weaknesses requiring senior management attention. At the time, the agency's CIO had been in place for only a short period. This official and the Director of USPTO began a concerted effort to improve the agency's information security program, including devoting more resources to it and working to improve policy, controls, and oversight. The results of their commitment are evident in a considerably improved information security program. (See page 14.)

Authority for IT investment decisions. (OMB Question B.2)

Significant IT Investments Require CIO Concurrence. No operating unit can make a major IT investment without the Department CIO's review and concurrence. The Commerce Information Technology Review Board, cochaired by the CIO and chief financial officer (CFO), was established to support IT investment decision making. Certain IT initiatives not necessarily reviewed by the board are also subject to the Department CIO's approval. All other significant IT investment proposals must be approved by the operating unit CIO. (See page 15.)

USPTO. A management council consisting of USPTO senior executives, including the CIO, reviews and approves the agency's budget, including IT investments. The council also must approve all new initiatives, including IT investments, having a life-cycle cost greater than $100,000. Only those IT investments with which the agency CIO concurs are brought before the council. (See page 15.)

Agency head's efforts to ensure that the information security plan is practiced throughout the life cycle of each system. Specific and direct actions taken by the agency head to verify that the unit's program officials and CIO are ensuring that security plans are up-to-date and practiced throughout the life cycle of each system. (OMB Questions B.3 and B.4)

Steps for Managing Life Cycle Information Security Are Prescribed in the Department's Policy. The Department's new policy delineates the requirements for managing information security for each system life-cycle phase and assigns primary responsibility to the system owner. Commerce has management and oversight processes to help ensure that life-cycle information security requirements are adhered to for all but one phase—disposal—for which it lacks an oversight mechanism. (See page 16.)

USPTO. USPTO's draft policy states that information security is managed throughout a system's life cycle, a responsibility assigned primarily to system owners. However, the policy does not contain a clear and concise delineation of requirements by life-cycle phase, nor does the agency's system life-cycle management manual (LCM). Both of these documents would be improved by the addition of such information so that program officials and system owners fully

understand their roles. The draft policy describes information security oversight reviews to be conducted by USPTO's CIO Office, and a technical review board appointed by the CIO is charged with evaluating systems and associated information security concerns at key system milestones. The certification testing conducted this past year identified areas throughout the system life cycle in which policies, procedures, and processes need to be improved. USPTO intends to revise its technical standards and guidelines and streamline its LCM next fiscal year to address these issues. (See page 16.)

Integration of information security program with critical infrastructure protection responsibilities and other security programs (e.g., continuity of operations, and physical and operational security), including efforts to eliminate unnecessary overhead costs and ensure that policies and procedures are consistent and complementary across the various programs and disciplines. (OMB Questions B.5 and B.6)

Information Security and Critical Infrastructure Protection Responsibilities Are Well Integrated, and Coordination With Other Security Functions Is Increasing. Commerce's critical infrastructure and information security programs are under the authority of the Department CIO and are highly integrated. The Department's policy delineates partnerships that must be maintained with offices under the CFO that have other security responsibilities, including the Office of Security (OSY), the Office of Human Resources Management, and the Office of Acquisition Management. (See page 19.)

USPTO. The agency's draft policy addresses coordination and cooperation between information security and other security programs, including interface with USPTO's physical security and human resource offices. USPTO has no national-critical assets. (See page 20.)

Agency's identification of its critical operations and assets (both national critical and mission critical) and the interdependencies and interrelationships of those operations and assets. (OMB Question B.7)

National- and Mission-Critical Asset Identification Efforts Continue to Be Refined. Commerce has identified its national-critical assets—an inventory it continues to update and refine—but has not determined the interdependencies among them. Both the Department and USPTO have identified and continue to refine their mission-critical asset inventory, and to the extent that security plans for these systems follow the required NIST guidance, they identify direct interconnections with other systems for information sharing. As the Department and USPTO define and document their enterprise architectures—which show the relationship between business functions and the technologies and information that support them—they should identify interrelationships of mission-critical systems. (See page 21.)

How agency head ensures that the agency and all its components have documented procedures for reporting security incidents and sharing information about common vulnerabilities. (OMB Question B.8)

The Department's Information Security Policy Has Requirements for Documenting Incident Reporting Procedures. The Department's policy defines the types of incidents that need to be reported and requires each operating unit to submit its response procedures to Commerce's CIO Office for review and approval. The policy requires operating unit computer incident response teams (CIRTs) and the Department's CIRT to report incidents to the Federal Computer Incident Response Center (FedCIRC), but does not set a timeframe for doing so. A memorandum of agreement between

OIG, CIO, and OSY—which will be revised and renewed in FY 2004—delineates roles, responsibilities, and procedures for reporting incidents to OIG and external law enforcement. The details of this agreement need to be incorporated into or referenced by the Department's information security policy. (See page 22.)

USPTO. USPTO has draft incident response procedures, which it intends to finalize by the end of the fiscal year. While detailed and specific, the procedures do not provide a timeframe for reporting incidents to FedCIRC or require notifying OIG when an incident occurs. The director of the IT Security Program Office told us that modifications will be made to address these areas before the procedures are finalized. (See page 23.)

The Department's Risk Assessments, Security Plans, and Testing of Security Controls Continue to Need Serious Attention. Our evaluation this year found many risk assessments and security plans that did not provide essential information for determining appropriate system security controls, and still others whose information was inaccurate or inconsistent. We also found that certifications were frequently granted without careful review of the documentation and with little or no testing, and thus did not identify residual risks.[7] Without reliable documentation and certifications, accrediting officials lack sufficient information for making informed decisions about whether a system's residual risks are acceptable and accreditation is therefore desirable. The deficiencies we identified affected systems controlled by program officials as well as by operating unit CIOs. According to the Department CIO, improvements are being made to the certification and accreditation process that should correct some of the problems we identified with the current accreditations. (See page 25.)

Risk assessments, security level determinations, security plans, and security control testing and evaluation. (OMB Question C.1)

USPTO Is Making Significant Improvements to Risk Assessments, Security Plans, and Testing of Security Controls. The agency's one certified and accredited system had a thorough risk assessment and comprehensive security and contingency plans. Certification included extensive testing of security controls that identified weaknesses in the system itself, as well as organization-wide security issues. USPTO appears to be using the same rigorous process for certifying and accrediting its remaining systems. It is clear that as the agency corrects the problems identified by means of its certification and accreditation program, its systems will be appreciably more secure. (See page 27.)

The agency CIO's ability to adequately maintain an agencywide information security program, ensure effective implementation of the program, and evaluate the performance of major agency components. (OMB Question C.2)

The Department CIO Continues to Make Progress in Improving Information Security Throughout Commerce. The Department CIO has focused intensely on improving information security and has made significant strides. In finalizing the new information security policy this past January, he gave Commerce a comprehensive blueprint for securing agency information systems. The Department CIO is making a determined effort to effectively implement the

[7]Residual risks are the risks remaining after appropriate security controls have been applied to the information system.

security program, though much remains to be done—especially in assessing risk, determining appropriate security controls, testing and evaluating these controls, and certifying and accrediting systems. But satisfying the demands of information security law, policy, and guidance requires substantial change in the culture of an organization that, until recently, has given scant attention to this area. Thus, it remains a considerable challenge to ensure that program and IT officials throughout the Department and personnel with specialized information security roles understand their responsibilities and have the knowledge and skills to carry them out effectively. The Department CIO Office is evaluating the performance of all Commerce operating units through a compliance review program designed to validate the security information they report and assess the effectiveness of their information security programs. (See page 28.)

USPTO. Last fiscal year, USPTO's newly appointed CIO began giving serious attention to improving information security and has made considerable progress. USPTO's information security policies, when refined and finalized, should address the requisite security program requirements. As we have discussed previously, USPTO is well on its way to certifying and accrediting all of its mission-critical systems and is using sound processes to do so. As with the rest of the Department, effectively implementing the required information security program at USPTO requires significant cultural change. USPTO's CIO is currently working with program officials to facilitate their understanding and acceptance of their more active role and increased accountability before the policy is finalized. We believe the CIO's effort is essential to initiating and maintaining an effective information security program.

The involvement in and oversight of USPTO's CIO Office in the ongoing certification and accreditation efforts, the POA&M process, and the work of an employee designated as an internal IT auditor are the principal means by which USPTO is evaluating its major components. The Department intends to assess USPTO as part of its compliance review program.
(See page 28.)

The agency CIO's efforts to ensure that all agency employees, including contractors and those employees with significant information security responsibilities, are aware of and trained in information security policies and practices. (OMB Question C.3)

Information Security Awareness Training Is Being Addressed, but Specialized Training Requirements Are Needed. The Department's policy includes requirements for security awareness training for new employees and contractors, and annual refresher training for all existing employees and contractors who have access to systems containing sensitive information. During this fiscal year, the Department CIO acquired an enterprise license for web-based information security training, which will make awareness refresher training available free of charge to Commerce employees and contractors. However, we found slow progress has been made in providing specialized training for personnel with significant information security responsibilities. The Department has been attempting to establish more uniform requirements or guidance for specialized training, and in the meantime, is making specialized training available throughout Commerce via the same enterprise license. Our independent evaluation this year found that some IT security officers and system administrators still lack a sufficient understanding of their duties and responsibilities. We also found a pervasive lack of understanding of the objectives and requirements of system risk assessment, security planning,

contingency planning, and certification and accreditation. These findings highlight the importance of ensuring that specialized security training is provided to those who need it. (See page 30.)

USPTO. USPTO is using the Department's enterprise license to provide the mandated annual awareness refresher training, and plans to implement specialized training for approximately 150 employees and contractors, also via the Department's license. USPTO executives have received specialized training in information security, including certification and accreditation, and CIO managers and staff have been trained in USPTO's IT processes, including information security. USPTO is using NIST guidance to develop requirements for specialized training. (See page 31.)

Agency CIO's efforts to fully integrate security into the capital planning and investment control process. (OMB Question C.4)

Integration of Security into the Capital Planning and Investment Control Process Is Improving. We reviewed FY 2004 capital asset plans for BIS, NESDIS, NOS, NWS, and NTIA (FY 2005 plans were not available when we conducted our fieldwork). In general, these plans provide more specific information than last year's plans on security requirements and how they are addressed. Some, however, still contained generic discussions of security requirements and controls, and it was unclear in one plan whether the system had been certified and accredited. All of the plans stated that the system's security controls had been tested. Our assessment found little if any testing of security controls for most systems beyond self assessments. (See page 32.)

USPTO. The agency prepared capital asset plans for the FY 2004 budget submission that comprehensively addressed the areas required by OMB and demonstrate that USPTO has made a serious effort to include information security in its capital asset planning. (See page 32.)

Conclusion

Conclusion. Our FY 2003 FISMA review found that senior management continues to give attention to information security. With the support of the Deputy Secretary, the Department's CIO has worked hard to improve information security throughout Commerce and has made noteworthy progress. The Department's new policy comprehensively defines Commerce's program for assuring agency information systems are adequately protected, and its detailed requirements are helping improve the security programs of the operating units.

This noteworthy progress is moderated by considerable challenges. The most difficult of these has been ensuring adequate security on the hundreds of Commerce systems—a challenge that cannot be fully met until program and IT officials throughout the Department better understand what is expected of them, and all personnel with specialized information security roles acquire and maintain the requisite knowledge and skills. (See page 33.)

USPTO. USPTO's information security program continues to progress. This agency is working to ensure that its senior program officials understand and accept their responsibilities for information security, a prerequisite for an effective and long-lived program. USPTO is well on its way to having systems certified and accredited. And because it is using a rigorous approach and comprehensive testing, it has gained a great deal of insight into system-specific weaknesses

that must be corrected and organization-wide security policies, procedures, and processes that must be improved. USPTO must continue to focus on correcting the identified system weaknesses; improve policies, procedures, and processes; and ensure compliance on a continuing basis. (See page 33.)

INTRODUCTION

The Federal Information Security Management Act (FISMA), set out in Title III of the E-Government Act of 2002 (P.L. 107-347), was signed into law on December 17, 2002. FISMA permanently reauthorized and expanded upon the framework laid out in the Government Information Security Reform Act of 2000 (GISRA),[8] for ensuring that information resources supporting federal operations and assets are protected by effective security controls. FISMA requires agencies to conduct annual information security program reviews and Offices of Inspector General (OIGs) to perform annual independent program evaluations.

As a performance-based organization, the United States Patent and Trademark Office (USPTO) has submitted its budget materials, information security review, and *Performance and Accountability Report* separate from those of the Department. For the past 2 fiscal years, we prepared a separate independent evaluation report on information security at USPTO. For fiscal year 2003, however, we are including USPTO in this single, Commerce-wide evaluation report, as is the Department in its OMB submission. This consolidation is in keeping with OMB's FY 2002 Report to Congress on federal government information security reform, in which it combined USPTO with the rest of Commerce. The details and results of our independent evaluation for FY 2003 follow below.

OBJECTIVES, SCOPE, AND METHODOLOGY

We sought to determine whether the Department of Commerce's (DOC's) information security program and practices for unclassified systems comply with the requirements of FISMA. Our evaluation is based on the results of the following OIG work:

1. Assessments of selected systems at the National Oceanic and Atmospheric Administration's (NOAA's) National Marine Fisheries Service (NMFS) and National Environmental Satellite Data and Information Service (NESDIS);

2. Audit of general controls of financial systems (reviewed as part of the Department's FY 2002 consolidated financial statement audit and the financial statement audits of the National Technical Information Service (NTIS) and USPTO);

3. Review of the status of issues identified at the National Institute of Standards and Technology (NIST) and USPTO in our in-depth evaluation of these organizations last year;

4. Review of risk assessments, security plans, contingency plans, security test and evaluation materials (test procedures and results), certification and accreditation[9] documents, capital

[8] GISRA expired in November 2002.
[9] Certification is the formal testing and evaluation of the security safeguards on 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.

asset plans (Exhibit 300s), and plans of action and milestones (POA&Ms)[10] for a range of systems in the Bureau of Economic Analysis (BEA), Bureau of Industry and Security (BIS), Census Bureau, International Trade Administration (ITA), NIST, NTIS, and National Telecommunications and Information Administration (NTIA), NOAA, and USPTO;

5. Interviews with the CIOs and senior information security officials of the Department, Census, ITA, NIST, NOAA, and USPTO to obtain additional information regarding the agencywide POA&M process and responsibilities of the agency head, operating unit heads, and agency and operating unit program officials and chief information officers (CIOs), and

6. Review of a random sample of 24 contracts at Census, NIST, NOAA, Office of the Secretary, and USPTO to assess the Department's progress in incorporating information security requirements into information technology (IT) service contracts.

We conducted our evaluation using FISMA; OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources"; *DOC IT Security Program Policy and Minimum Implementation Standards*; the *National Information Assurance Certification and Accreditation Process (NIACAP)*[11]; and the following NIST special publications: *Security Self-Assessment Guide for Information Technology Systems* (800-26), *Risk Management Guide for Information Technology Systems* (800-30), *Guide for Developing Security Plans for Information Technology Systems* (800-18), and *Contingency Planning Guide for Information Technology Systems* (800-34). OIG contractors conducted the general control reviews of financial systems against criteria contained in GAO's *Federal Information System Controls Audit Manual* (FISCAM).

The structure and content of this report are designed to be responsive to the guidance provided by OMB in *Reporting Instructions for the Federal Information Security Management Act,* while also providing useful information for Commerce officials. As directed in this guidance, we begin with question A.2.a. We are issuing our report in final because it makes no new recommendations.

We performed this evaluation 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. We conducted our fieldwork between October 2002 and August 2003.

[10] OMB guidance directs agencies to develop plans of action and milestones (POA&Ms) to remediate program- and system-level IT security weaknesses and track each deficiency until it is corrected.
[11] National Security Agency, *National Information Assurance Certification and Accreditation* Process (NIACAP), National Security Telecommunications and Information Systems Security Instruction No. 1000. NIACAP establishes the minimum standards for certifying and accrediting national security systems. Its use is required by the Department's information security policy for sensitive but unclassified systems.

Overview of FISMA IT Security Review

Total number of programs, systems, and contractor operations or facilities evaluated in FY 2003. (OMB Question A.2.a)

In FY 2003 we assessed a total of 43 systems in 9 of the Department's 14 operating units (see table 1), and 24 contracts in 5 of those operating units.

Table 1. Operating Unit Systems Assessed in FY 2003

Office of the Secretary
Commerce Administrative Management System*
Bureau of Economic Analysis (BEA)
National Income and Wealth Division
Industry Economics Division
Local Area Network
Bureau of Industry and Security (BIS)
Export Control Automated Support System
Bureau Communication Infrastructure
Treaty Compliance/Information Management System #1
Census Bureau
National Processing Center
Geography
Data Centers*
Economic Development Agency (EDA)
Data Center*
National Institute of Standards and Technology (NIST)
Manufacturing Engineering Laboratory Office System
Time Scale and Network Time Services
Network Infrastructure (Gaithersburg)
Network Infrastructure (Boulder)
Boulder E-mail Server System
Data Center*
National Technical Information Service (NTIS)
Automated Document Storage and Retrieval
Computing Information Service Publishing
PC and Network
Data Center*
United States Patent and Trademark Office (USPTO)
Network Perimeter System
Financial Management Systems*

National Oceanic and Atmospheric Administration (NOAA)
NOAA Headquarters
Data Center*
National Environmental Satellite Data and Information Service (NESDIS)
Headquarters Local Area Network
Research Data System
Integrated Program Office Local Area Network
National Marine Fisheries Service (NMFS)
Headquarters Local Area Network
Headquarters Wide Area Network
National Ocean Service (NOS)
Coastal Services Center IT Support System
Nautical Charting System
Office of Coast Survey Support Hydrographic Support Sys.
National Weather Service (NWS)
NOAA Weather Radio
WSR-88D Weather Radar (NEXRAD)
Advanced Weather Interactive Processing System
Kansas City Weather Forecast Office
Salt Lake City Weather Forecast Office
Kansas City River Forecast Center
National Centers for Environmental Prediction
Office of Oceanic and Atmospheric Research (OAR)
Office of Global Programs
NOAA Profiler Network Central Facility
Space Environment Center
Boulder Campus Network

*Review of IT Controls to Support the FY 2002 Consolidated Financial Statement Audit

FINDINGS

Information security in IT service contracts. (OMB Question A.2.b-e)

I. Information Security in IT Service Contracts Is Improving, but Additional Efforts Are Needed

In fiscal year 2002, Commerce's IT expenditures totaled nearly $500 million (43 percent of all its contract obligations). More than two-thirds of that amount (approximately $334 million) was for IT services. In the absence of rigorous security provisions in contract documents, this heavy reliance on contractor services leaves Commerce systems and data highly vulnerable to security violations.

In support of our FY 2002 independent evaluation, we reviewed 40 contracts[12] awarded by several operating units including USPTO. Across the board, we found the contracts had either insufficient security provisions or none at all, and we concluded that federal and departmental policy and guidance for incorporating such provisions were lacking.

In the intervening year, the Department issued a new information security policy, which emphasizes that IT security officers, system owners,[13] contracting offices, and contracting officers' technical representatives (COTRs) must work together to ensure that information security is addressed throughout the acquisition process, and provides guidance on monitoring contractors who have access to departmental systems and data. To support these requirements, the CIO Office, the Office of Acquisition Management (OAM), and the Office of Human Resources Management (OHRM) have developed a security training module for procurement professionals, which is undergoing departmental review. In an April 2003 amendment to a policy memorandum, OAM reemphasized the need for including information security provisions in contracts.

OAM has also drafted a standard contract provision for safeguarding the security of unclassified systems and information, which is also undergoing department review.[14] The provision requires, among other things, a system security plan and certification and accreditation for contracted IT resources/services that involve connection to Commerce networks or storage of Commerce data on contractor-owned systems. OAM's assessment of current contracts and solicitations identified more than 300 needing modification to incorporate appropriate security provisions. However, OAM is not planning to advise contracting officers to modify the deficient contracts until the draft provision is issued in final. With no date for issue set, we are concerned by the absence of interim action to mitigate security risks posed by these contracts.

---

[12] The term "contract" includes task orders and delivery orders issued under multiple award contracts and government-wide agency contracts (GWACs).

[13] The Department's information security policy defines a system owner as a project manager with day-to-day management and operational control over the system and direct oversight of the system/network administrators and operations staff.

[14] Similarly, the Civilian Agency Acquisition Council is working on a draft change to the Federal Acquisition Regulation that would ensure that information security is included in IT acquisitions, but the timeframe for its completion is unclear.

Although a formal provision has not been completed, our FY 2003 independent evaluation did note some progress in incorporating security into IT service contracts. Our review of 24 contracts awarded during this fiscal year by the Office of the Secretary, NOAA Headquarters, NIST, Census, and USPTO found that contract documents contained at least minimal provisions for security. Contracts typically require risk and suitability assessments and background clearances for contractors working in government facilities; and some require contractors to attend security awareness training and follow information security procedures.

However, we found only two contracts that contained most of the elements of the draft provision. In addition, we found little evidence of appropriate review of contractor compliance with security requirements, or of contracting staff working with COTRs and information security offices—as mandated in the Department's new policy—to ensure that security is addressed during development of contract requirements and statements of work. We believe the general absence of such provisions and the inadequate interface among all staff involved in the contracting/IT security process continue to place Commerce systems and data at risk.

Contracts should improve once OAM's standard provision is finalized and contracting staff are trained to use it. However, it is essential that communication improve among contracting, technical, and information security staffs when planning, executing, and administering contracts that include IT services. These personnel have significant management and oversight responsibility, and they must work as a team to ensure that security is adequately addressed in contract planning and development of requirements and performance measures, so that contractor accountability may be established. They must also work together to assess contractor compliance with security requirements, and document contract files accordingly.

II. The Department Is Continuing to Refine Its Systems Inventory

Agency's work to develop an inventory of major IT systems. (OMB Question A.2.f)

In January 2003, the Department issued an updated and expanded information security policy that provides comprehensive requirements and direction for the operating units in conducting their own information security programs. The Department views system inventory control as the foundation for managing the information security program, and the policy requires all operating units to maintain a comprehensive inventory of classified and unclassified IT systems that provides security information (including dates for the most recent risk assessment, security plan approval, contingency plan and related testing, certification and accreditation, and self-assessment). It also must include the dates of audits performed by external entities such as OIG, the General Accounting Office (GAO), or the Department within the previous 12 months. All operating units including USPTO must provide a copy of their inventory to the Department's IT security program manager twice a year.

Commerce's CIO Office is reviewing the inventory data as part of its compliance review program, which is designed to validate the security information reported by operating units and assess the effectiveness of their information security programs. This year's inventory review is focusing on whether operating units are properly applying NIST criteria in defining system boundaries. (The Department's intent is to review information security for all systems over a 3-year cycle. To streamline information security management, particularly the certification and accreditation process, some operating units have reassessed system boundaries and redefined systems, thereby significantly reducing their inventories. For example, in FY 2002, the Department reported that Census had 82 systems; the March 2003 system inventory identifies only 8 Census systems. While it is appropriate to define systems in a way that facilitates their administration, it is important that the definitions be logical and meaningful and that Department and operating unit management have sufficient information about the number and type of IT assets in the organization.

Material weaknesses. (OMB Question A.3)

III. The Department Should Continue to Report Information Security as a Material Weakness

FISMA requires that significant deficiencies in information security policy, procedures, or practices be reported as material weaknesses. OMB Circular A-130 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. For the past 2 fiscal years, the Department reported information security as a material weakness in its Accountability Report. In our independent evaluation last year, we stated that the Department should continue to report information security as a material weakness until all systems that are national critical (part of the critical infrastructure) and mission critical have been certified and accredited. The Department established a goal of certifying and accrediting these systems by the end of FY 2003.

As discussed in Finding XI, in this year's evaluation we that found numerous systems reported as certified and accredited have significant deficiencies in their certification and accreditation materials. For example, we found risk assessments and security plans that have no basis for determining appropriate security controls; identify sensitivity levels that are not commensurate with the requirements for confidentiality, integrity, and availability of the information handled; and do not fully and accurately describe the system environment and interconnections. In most cases, there was no evidence that security controls had been tested. We also found systems that had either no contingency plans or whose plans specified no measures for recovering IT services following an emergency or system disruption. Few contingency plans had evidence of testing. These problems call into question the effectiveness of the certification and accreditation processes being used.

The Department's new policy requires compliance with the National Information Assurance Certification and Accreditation Process (NIACAP), which establishes minimum certification and accreditation standards. The operating units are currently working to improve the content and quality of their certification and accreditation processes and materials to comply with NIACAP, and some units are attempting to rework existing certifications and accreditations by September 30, including some that we reviewed.[15]

Given the shortcomings in the systems we evaluated, however, we do not believe that certification and accreditation of the Department's roughly 340 national-critical and mission-critical systems[16]—of sufficient quality and content—can be completed by the end of the fiscal year. Thus, while the Department should be commended for its focused efforts to certify and accredit, we believe that information security should be reported as a material weakness for FY 2003. We have worked closely with the Department CIO on information security concerns throughout the year, and he has indicated agreement with our conclusion.

[15] We obtained certification and accreditation materials from the operating units in June and July 2003.
[16] The number of systems is based on the Department's March 2003 system inventory.

USPTO

As noted earlier, USPTO submits its Accountability Report separate from the rest of the Department. Last year we found that the agency lacked current certifications and accreditations for its systems and suggested that it report information security as a material weakness until its mission-critical systems are certified and accredited. (USPTO has no systems designated as national critical). USPTO reported information security as a material weakness in its FY 2002 Accountability Report. In response to last year's evaluation, the agency indicated that it would rank its systems by risk and criticality, and certify and accredit all high-risk systems by the end of FY 2003, and the balance by the end of FY 2004.

The agency subsequently revised its systems inventory by consolidating more than 100 systems into 19 systems, 9 mission critical and the remainder business essential. It planned to have its 9 mission-critical systems and 1 classified system certified and accredited by the end of FY 2003. As of mid-September, all 10 systems had undergone certification testing, 5 had been granted interim accreditations, and 1 had received final accreditation. USPTO expects to grant the remaining 4 systems 120-day interim accreditations by the end of the fiscal year. USPTO is employing a sound certification and accreditation process that includes rigorous testing of security controls. Interim accreditations are not granted without comprehensive security plans, testing, and risk assessments, with final accreditations given after problems identified in certification testing have been corrected.

As discussed in Finding XI, our review of USPTO's certification and accreditation materials demonstrates that it has made an extremely conscientious effort to employ a disciplined process according to the NIACAP standard, including rigorous testing of security controls. And this process has been effective: it has identified numerous risks that must be addressed before all systems receive full accreditation. We reported in last year's evaluation that the Director of USPTO has made a commitment to protect the bureau's information assets; the certification and accreditation program, under the leadership of USPTO's CIO, confirms this commitment. But because of the risks identified and the lack of final accreditations, we believe that USPTO should report information security as a material weakness for FY 2003.

IV. The Department Has Established a Sound Plan of Action and Milestone (POA&M) Process

Agencywide plan of action and milestone process. (OMB Question A.4)

FISMA requires each agency to develop, document, and implement an information security program that includes a remedial process for addressing any deficiencies in its information security policies, procedures, and practices. OMB guidance states that agency program officials must develop, implement, and manage corrective action plans, referred to as POA&Ms, for all systems that support their operations and assets. It also states that CIOs must develop, implement, and manage corrective action plans for all programs and systems they operate and control.

The requirements for POA&Ms are specified in the Department's new information security policy and are responsive to the criteria contained in OMB's FY 2003 FISMA guidance. The Department develops, implements, and manages POA&Ms for all of its systems that have identified security weaknesses. System owners are required to prepare the POA&Ms for their systems, and the operating unit IT security officer prepares the POA&M for the unit's program. Operating units are required to submit their POA&Ms, including the status of corrective actions, to the Department CIO Office monthly.

The Department monitors POA&Ms closely and uses them to manage corrective actions for all identified weaknesses. Our reviews at Census, ITA, NIST, and NOAA indicate that POA&Ms in these operating units are being implemented in accordance with the Department's guidance. OIG has access to all POA&Ms, but because many are based primarily on self-assessments, which may not identify all weaknesses, we place greater reliance for identifying weaknesses on independent reviews. Commerce's POA&M database does not include the accounting codes associated with each line of the IT budget request, and IT system and budget reviews do not formally take into account the content of the POA&Ms, although attention is given to information security in these reviews. Commerce plans to tie POA&Ms to the system budget request in FY 2004. Our evaluation of the Commerce's process against OMB's criteria is presented in table 2.

USPTO

Like the Department, USPTO develops, implements, and manages POA&Ms for systems that have identified security weaknesses. The agency's CIO Office develops the POA&Ms, collaborating with program officials to ensure that information security weaknesses are addressed. The CIO closely monitors the POA&Ms and uses them to manage corrective actions for identified weaknesses. OIG has access to all POA&Ms, but relies more heavily on independent reviews. To satisfy OMB's guidance, program officials at USPTO need to have primary responsibility for the POA&Ms for systems that support their operations. USPTO has been submitting its POA&Ms directly to OMB; beginning in FY 2004, it will submit them to the Department CIO Office for incorporation into Commerce's consolidated report to OMB. Table 3 presents our evaluation of USPTO's process against OMB's criteria.

Table 2: Evaluation of Department's POA&M Process

OMB FISMA Criteria	Criterion Met? (Y/N)	OIG Evaluation
Agency program officials develop, implement, and manage POA&Ms for every system under their responsibility with noted IT security weaknesses.	Y	Program officials must record in POA&Ms any deficiencies found through an external review, internal self-assessment, or compliance review, and must track corrections to completion.
Agency program officials report at least quarterly to the CIO on their remediation progress.	Y	Reporting is monthly.
Agency CIO develops, implements, and manages POA&Ms for every system under their responsibility with noted IT security weaknesses.	Y	Operating unit CIOs must record in POA&Ms any deficiencies found through an external review, internal self-assessment, or compliance review, and must track corrections to completion.
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.	Y	The Department CIO centrally tracks and maintains all POA&M activities on a monthly basis.
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	Y	The POA&Ms contain all known security weaknesses, are closely monitored by the Department, and are used to manage corrective actions. Because many POA&Ms are based primarily on self-assessments, which may not identify all weaknesses, OIG places greater reliance for identifying weaknesses on independent reviews.
System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) so as to justify IT security funds in the budget process.	N	The Department plans to ensure that POA&Ms are tied to the system budget request in FY 2004, but does not do so currently.
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.	Y	All weaknesses identified by OIG are included in corrective action plans. OIG has access to all POA&Ms.
The agency's POA&M process prioritizes agency IT security weaknesses to ensure that significant weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.	Y	A formal prioritization process does not exist. However, reviews of POA&Ms at the operating unit and Department level appear to ensure that significant weaknesses are addressed in a timely manner.

Table 3: Evaluation of USPTO's POA&M Process

OMB FISMA Criteria	Criterion Met? (Y/N)	OIG Evaluation
Agency program officials develop, implement, and manage POA&Ms for every system under their responsibility with noted IT security weaknesses.	N	All weaknesses found through an external review, internal self-assessment, or compliance review are recorded in POA&Ms. However, program officials do not develop the POA&Ms. Rather, they are developed by the CIO Office, in collaboration with program officials.
Agency program officials report at least quarterly to the CIO on their remediation progress.	Y	USPTO's CIO works collaboratively with program officials to track remediation progress. Reporting is quarterly.
Agency CIO develops, implements, and manages POA&Ms for every system under their responsibility with noted IT security weaknesses.	Y	USPTO's CIO records in a POA&M any deficiencies found through an external review, internal self-assessment, or compliance review.
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.	Y	USPTO's CIO centrally tracks and maintains all POA&M activities quarterly.
The POA&M is the authoritative agency and IG management tool for identifying and monitoring agency actions to correct information and IT security weaknesses.	Y	The POA&Ms contain all known security weaknesses, are closely monitored by USPTO, and are used to manage corrective actions. Because many POA&Ms are based primarily on self-assessments, which may not identify all weaknesses, OIG places greater reliance for identifying weaknesses on independent reviews.
System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.	Y	As of its September 2003 submission, USPTO's POA&Ms have unique identifiers that link them to the appropriate system budget request.
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.	Y	All weaknesses identified by OIG are included in USPTO's corrective action plans. OIG has access to all POA&Ms.
The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.	Y	USPTO's CIO reviews the POA&Ms monthly to track progress and determine priorities.

Responsibilities of Agency Head

Steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials, and actions to implement and enforce these steps. (OMB Question B.1)

V. Responsibilities and Authorities Are Clearly Specified for the Department CIO and Operating Unit Officials

The responsibilities and authorities for the Department's CIO and program officials have been clearly specified in the new information security policy. This policy, is part of the Department's *Information Technology Management Handbook,* which details and clarifies the CIO's authorities set forth in Department Organization Order (DOO) 15-23, "Chief Information Officer." It was through this order that the Secretary delegated to the CIO responsibility for developing and implementing a departmental information security program to ensure the confidentiality, integrity, and availability of IT resources. The handbook is itself a DAO and is thus the authority for policies and regulations regarding IT resource management throughout Commerce.

Department CIO. The new policy makes the Department's CIO responsible for overseeing Commerce's information security program; ensuring an appropriate level of protection for all departmental information resources; issuing policy and guidance that establish a framework for an information security program for the Department and its operating units; ensuring that funding and resources are committed for the program's staffing, training, and support and for implementing system safeguards; and monitoring, evaluating, and reporting to the Deputy Secretary on the status of information security within the Department.

FISMA requires agency heads to delegate to their CIO the authority for ensuring compliance with the Act. In a recent decision memorandum, the Secretary explicitly delegated the requisite authorities to the Commerce CIO. The specific authorities are that the CIO (1) designate a senior agency information security officer; (2) develop and maintain an agencywide information security program, as well as information security policies, procedures, and control techniques; (4) train and oversee personnel with significant responsibilities for information security; and (5) provide assistance to senior agency officials concerning their information security responsibilities.

Operating unit heads. The policy gives operating unit heads explicit responsibility for their unit's information security. Unit heads are required to communicate to all employees the importance of information security to the unit's and Department's mission; assign management of IT systems to responsible program officials (e.g., heads of line offices and major operating unit components); ensure that the operating unit has an established information security program to protect its systems; and serve as the designated approving official (DAA)[17] for systems that support the operating unit's mission. (DAA authority may be delegated to a program official.)

[17] The DAA is the official with the authority to accredit systems, i.e., formally assume responsibility for operating a system at an acceptable level of risk.

Program officials. The policy charges program officials—members of an operating unit's top-level management team (e.g., heads of line offices and directors of major operating unit components)—with ensuring implementation of an effective information security program for the systems they oversee; assigning responsibility for daily system operations and security to system owners; serving as the DAA, when so designated by the unit head, for systems that support the operating unit's mission; and ensuring availability of adequate resources for implementing IT security activities.

The Commerce-wide information security program, which is overseen by the Department's CIO, provides the foundation for enforcing unit responsibilities and authorities. This program requires each operating unit to have its own information security program and documented policy that conform to departmental policy. The Department CIO's responsibilities and authorities are, in turn, enforced through his reporting on information security to the Deputy Secretary.

As we have noted in our previous independent evaluations, the Secretary issued an information security memorandum in July 2001 to secretarial officers and heads of operating units, in which he gave greater specificity to these officials' responsibilities, and charged them with assuring compliance with information security directives. The memorandum stated that information security should be given high priority and sufficient resources and that secretarial officers and unit heads are expected to personally invest the time needed to achieve and maintain full compliance with information security improvement directives coming from the Department's newly developed IT management restructuring plan. This plan was designed to enhance the authority and effectiveness of operating unit CIOs. One of its provisions was that unit heads (or their designee) must establish CIO performance plans and evaluate this official's performance in consultation with the Department CIO. This requirement further helps ensure that information security receives the requisite attention.

At the end of last fiscal year, the Deputy Secretary highlighted to operating unit heads the information security improvements needed in their organizations: accompanied by the CIO and chief financial officer (CFO), the Deputy Secretary reviewed unit heads' progress toward meeting the President's Management Agenda, addressing information security and related weaknesses in light of the agenda's E-Gov component.

Over the past 2 years, the Deputy Secretary has reinforced the Secretary's emphasis on information security, and provided the Department CIO with strong support for its improvement. Indeed, we believe the progress made by Commerce in information security is attributable not only to the formal authority granted to the CIO position and the vigorous efforts made by the Department CIO, but also to the Deputy Secretary's support, which has significantly enhanced the CIO's effectiveness. Simply stated, operating unit heads understand that information security is a priority for the Deputy Secretary and that they need to be responsive to issues raised by the Department CIO.

In addition, corrective actions at NIST demonstrate that operating unit heads are better recognizing their new responsibilities. Last year we performed an in-depth review of NIST's information security program, which identified numerous weaknesses. In response to our findings, the NIST director took significant improvement actions. This year, we found that NIST

has made excellent progress in responding to our concerns and improving its information security program. As we recommended, NIST has established a CIO organization and appointed a full-time CIO; is improving its information security policies, including its policy for certification and accreditation; has refined its systems inventory; is working to track collaborators and researchers who are not on NIST campuses but who use NIST computing resources; and is implementing a capital planning and investment control process for IT.

USPTO

The responsibilities and authorities for USPTO's CIO and program officials are delineated in Agency Administrative Order 212-4, *Information Technology Security*, as are the responsibilities for the CIO Office to ensure the policy is implemented and enforced. At the time of our fieldwork, this policy was in draft, but was expected to be finalized by the end of the fiscal year. The draft policy addresses FISMA's requirement that heads of agencies accord the CIO the authority to ensure compliance with the Act by stating that the USPTO Director has delegated responsibility for all information security policies to the USPTO CIO. Currently, the CIO is working with senior program officials to ensure they understand their responsibilities for information security and to address any related concerns they may have. In the meantime, the policy is being refined to ensure that roles and responsibilities are clear and that its provisions comply with OMB Circular A-130 and FISMA.

In our independent evaluation last year, we reported that USPTO had long-standing information security weaknesses requiring senior management attention. The agency's CIO had been in place a short period of time when we began our work. After we brought our concerns to his attention, he and the agency's director began a concerted effort to improve the information security program, including devoting more resources to it and working to upgrade policy, controls, and oversight. The results of their effort are evident in a considerably enhanced program.

VI. Significant IT Investments Require CIO Concurrence

Authority for IT investment decisions. (OMB Question B.2)

No operating unit can make a major IT investment without the Department CIO's review and concurrence. The Commerce Information Technology Review Board (CITRB), cochaired by the CIO and CFO, was established to support IT investment decision making. The Department CIO, with input from the board, recommends to the Secretary and Deputy Secretary, through the Office of Budget, whether a proposed IT project should be funded. His FY 2005 budget guidance to operating unit CIOs emphasized that effective information security remains an important factor in the board's consideration of budget requests and provided the criteria against which the board evaluates a request's information security content.

The board evaluates new and ongoing IT investments designated by the Department's CIO. Systems are designated for review if they merit special attention due to their sensitivity, mission criticality, or risk; if their resources are shared among operating units; or if their life cycle cost exceeds $25 million. The board must also review IT projects costing more than $10 million and requiring a contract, as well as selected smaller projects, before the acquiring operating unit can receive authority to make a contractual commitment. According to the CIO, greater emphasis is being placed on information security in contracts in these reviews. The board periodically reviews the status of approved projects, and the CIO, in turn, uses the results of these reviews to recommend whether a project should be continued, modified, or terminated.

Other IT initiatives that meet certain thresholds must prepare capital asset plans (Exhibit 300) subject to the Department CIO's approval, but do not necessarily go before the board. For operating units without approved strategic and operational IT plans, this threshold is $500,000 in life-cycle costs. Operating units and NOAA line offices with approved plans have a threshold of $10 million, and the threshold for NOAA line offices without approved plans is $2.5 million. All other significant projects must be approved by the operating unit CIO.

USPTO

In July 2003, USPTO's CIO issued a draft IT capital planning and investment control process guide to provide a structured, integrated process for managing IT investments. The planning and control process is intended to ensure that all IT investments align with the agency's mission and strategic plan, and support business needs while minimizing risks and maximizing returns throughout the investment's life cycle. A management council consisting of USPTO senior executives, including the CIO, reviews and approves the agency's budget, including IT investments. The council also must approve all new initiatives, including IT investments, having a life-cycle cost greater than $100,000. Only those IT investments with which the agency CIO concurs are brought before the council.

Agency head's efforts to ensure that the information security plan is practiced throughout the life cycle of each system. Specific and direct actions taken by the agency head to verify that the unit's program officials and CIO are ensuring that security plans are up-to-date and practiced throughout the life cycle of each system. (OMB Questions B.3 and B.4)

VII. Steps for Managing Life Cycle Information Security Are Prescribed in the Department's Policy

The Department's new information security policy delineates the requirements for managing information security throughout the life cycle of each system.

The policy identifies five life-cycle phases: (1) initiation, (2) development/acquisition, (3) implementation, (4) operation and maintenance, and (5) disposal. Specific information security requirements must be met at each phase and are the responsibility of the system owner, with support from the appropriate IT security officer and CIO. Commerce has management and oversight processes to help ensure that life-cycle information security requirements are adhered to at phases 1 through 4, but lacks such an oversight process for phase 5—disposal. (See table 4.)

In the initiation phase, Commerce requires system owners to (1) obtain identifiers from the Department CIO that permits systems tracking in the Department-wide inventory, and (2) determine the sensitivity level[18] of the data processed by the system and the criticality of the system to the Department's mission. Responsibilities in the development/acquisition stage include determining system security requirements; performing a risk assessment; preparing the security plan, contingency plan, and test plan; and ensuring security in IT acquisitions. During implementation, certification and accreditation must occur before the system becomes operational. In the operation and maintenance phase, the system owner must ensure that the security plan is maintained, the contingency plan is updated and tested, vulnerability testing is performed, configuration management is carried out, security controls are periodically assessed, system logs are examined, and the system is recertified and reaccredited every 3 years. In the disposal phase, the system owner must see that federal records are properly preserved and archived, sensitive information is removed, and system components are destroyed or recycled appropriately.

USPTO

USPTO's draft policy states that information security is managed throughout a system's life cycle, gives this responsibility primarily to system owners and secondarily to developers, and identifies 6 life-cycle phases: (1) initiation, (2) concept, (3) detailed analysis and design, (4) development, (5) deployment, and (6) operations (including disposal). The draft policy does not identify or describe the requirements of each phase, but instead refers for guidance to USPTO's *Life Cycle Management Manual* (LCM) and *Life Cycle Certification and Accreditation Checklist TSG.* [19] Both of these documents would be improved by a concise description of life-cycle responsibilities so that program officials and system owners clearly understand their life cycle information security duties and responsibilities. Such clarification would also facilitate

[18] Sensitivity levels define the requirements for system confidentiality, integrity, and availability.
[19] A TSG is a technical standard or guideline.

Table 4. Departmental Management and Oversight Processes That Promote System Life Cycle Information Security

Life-Cycle Phase	Principal Management or Oversight Processes	Areas Addressed by Management and Oversight Processes
Initiation	• Inventory identifier request • CITRB reviews • Evaluations by operating unit IT review boards • Department and agency CIO reviews of capital asset plans	• Tracking of system security status. • Whether (a)information security is being planned and funded as part of the system architecture, (b) risks are well managed, and (c) privacy and confidentiality are being protected.
Development/Acquisition	• CITRB reviews • Evaluations by operating unit IT review boards • Department and agency CIO reviews of capital asset plans	• Whether (a) information security is being implemented and funded appropriately, (b) risks are well managed, and (c) privacy and confidentiality are being protected.
Implementation	• Certification and accreditation • CIO's compliance review program	• Whether system security safeguards have been implemented and meet applicable requirements and specifications. • Whether appropriate management official has formally authorized system operation and has explicitly accepted any residual risk.
Operation and Maintenance	• Recertification and reaccreditation at least every 3 years • CIO's compliance review program	• Whether system security safeguards are current and continue to meet applicable requirements and specifications. • Whether appropriate management official has formally reauthorized system operation and has explicitly accepted any residual risk.
Disposal	• None. Disposal requirements are contained in the Department's information security policy and security manual, but oversight processes are not identified.	

oversight. USPTO's CIO recognizes that the LCM needs to be streamlined and plans to see that it is next fiscal year.

This past year's certification testing has identified various areas throughout the system life cycle in which policies, procedures, and processes need to be improved. The contractor supporting the certification and accreditation program has been tasked to draft improvements to USPTO's technical standards and guidelines to accomplish this. This work is expected to be performed early next fiscal year.

To help ensure that security policies and procedures are followed through the life cycle of each system, the draft policy gives the director of the IT Security Program Office responsibility for managing reviews and inspections that examine (1) effectiveness of security control measures; (2) compliance with policies, procedures, standards, and guidelines; and (3) the user

community's awareness of security and related policies. The draft policy provides guidelines for settling policy violations, and its requirements for certification and accreditation help ensure appropriate life cycle system security management.

Another enforcement action taken by USPTO's CIO has been to designate an employee in the CIO's Office to act as an internal IT auditor. This employee reports to the Deputy CIO and is charged with performing such tasks as security documentation review and unannounced penetration testing of USPTO's networks and systems. In addition, the IT Security Program Office director—through USPTO's change control board—reviews proposed system changes and has the authority to reject change requests that would adversely affect information security. Finally, a technical review board appointed by the CIO reviews systems and associated information security concerns at key milestones.

VIII. Information Security and Critical Infrastructure Protection Responsibilities Are Well Integrated, and Coordination With Other Security Functions Is Increasing

Integration of information security program with critical infrastructure protection responsibilities and other security programs (e.g., continuity of operations, and physical and operational security), including efforts to eliminate unnecessary overhead costs and ensure that policies and procedures are consistent and complementary across programs and disciplines. (OMB Questions B.5 and B.6)

Commerce's critical infrastructure and information security programs are under the authority of the Department CIO and are highly integrated. The program manager for critical infrastructure protection (CIP) has responsibilities that require close coordination with the program manager for information security, such as responsibility for computer incident response capability (in concert with the Department's Office of Security and OIG). In turn, the IT security manager gives priority to systems considered national critical in compliance reviews of information security. These two program managers cochair the IT Security Coordinating Committee, a forum for information exchange and action on Department-wide security policies, problems, and potential solutions. A pending reorganization of the Department CIO Office will put the IT security and CIP managers under the same senior executive, and thus further solidify their partnership and interface.

Because Commerce has complied with the Clinger-Cohen Act requirement that the CIO report to the agency head and have IT as his primary responsibility, the Department necessarily has separate staffs to carry out other security functions. These functions—continuity of operations planning, physical security, and personnel security—come under the authority of the CFO. The Department's information security policy delineates partnerships that must be maintained by the CIO Office with offices under the CFO, including the Office of Security (OSY), OHRM, and OAM.

The CIO is currently working with these offices to ensure that IT personnel have appropriate suitability checks and background investigations before they are given access to Commerce systems, and to require that positions for network and system administrators, system developers, and information security program personnel, such as IT security officers and IT security managers, are designated as high risk. The CIO is responsible for the IT component of the continuity of operations plan, and thus works on the plan with the CFO's office. At present, emphasis is on ensuring there are backup sites for the Office of the Secretary and that the IT backup is tested. The Department CIO reports that the IT portions of the operating units' continuity of operations plans have been maturing, and he intends to review them in FY 2004.

As we have reported previously, the CIO Office, OSY, and OIG entered into a memorandum of agreement (MOA) in FY 2001 to define their respective roles and responsibilities relating to the development, implementation, and management of Commerce's information security program. This agreement was intended to promote a partnership among the three offices that both guarantees complete coverage of information security matters and prevents wasteful duplication

of effort. However, the MOA was scheduled to expire in November 2002, with the sunset of GISRA. These offices plan to modify the MOA and renew it in FY 2004.

USPTO

The agency's draft policy addresses coordination and cooperation between information security and other security programs. The director of the CIO's IT Security Program Office is responsible for coordinating matters of physical security for IT resources with the USPTO physical security office. USPTO's Office of Human Resources must inform new employees about the agency's information security practices, assist managers with disciplinary actions for policy violations, and notify the CIO Office of new and departing employees for account management purposes. The CIO Office works with the physical security office on the information security portion of USPTO's continuity of operations plan.

Agency's identification of its critical operations and assets (both national critical and mission critical) and the interdependencies and interrelationships of those operations and assets. (OMB Question B.7)

IX. National- and Mission-Critical Asset Identification Efforts Continue to Be Refined

The Department has identified its national-critical assets, and continues to update and refine this inventory. Using the Project Matrix methodology,[20] the Critical Infrastructure Assurance Office (CIAO) had helped Commerce identify national-critical assets, and was also supporting an assessment of interdependencies. However, since the CIAO's move from Commerce to the Department of Homeland Security during this fiscal year, efforts to complete the assessment have ceased. Department officials told us that the Project Matrix methodology has been abandoned by the CIAO and a new methodology is being developed. As noted previously, USPTO has no national-critical systems.

The Department and USPTO have identified their mission-critical assets, and continue to refine this inventory, as well. To the extent that security plans for these systems follow NIST guidance, they identify direct interconnections with other systems for information sharing. As the Department and USPTO define and document their enterprise architectures—which show the relationship between business functions and the technologies and information that support them— they should identify interrelationships of mission-critical systems.

[20] Project Matrix has been used to determine the assets and transportation/transmission links essential to meeting responsibilities of the federal government that are deemed "critical"–that is, their incapacitation could jeopardize the nation's security, seriously disrupt the functioning of the national economy, or adversely affect the health or safety of large segments of the American public. The methodology involves a two-step process in which each civilian federal department and agency identifies (1) its nationally critical functions and services, and (2) the assets and links required to perform or provide them.

X. The Department's Information Security Policy Has Requirements for Documenting Incident Reporting Procedures

How agency head ensures that the agency and all its components have documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. (OMB Question B.8)

FISMA requires agencies to have documented procedures for detecting, reporting, and responding to security incidents, including steps for notifying and consulting with the Federal Computer Incident Response Center (FedCIRC), appropriate law enforcement agencies, and relevant OIGs when incidents occur. It also requires agencies to ensure compliance with minimally acceptable system configuration requirements. According to OMB, this provision encompasses traditional system configuration management, employing clearly defined system security settings and maintaining up-to-date patches[21].

Incident Handling and Reporting

Our first independent evaluation in FY 2001 found that only 4 of the Department's 14 operating units—Census, NOAA, NIST, and USPTO—had established a computer incident response team (CIRT). Last fiscal year, Commerce expanded coverage throughout the Department by creating the DOC CIRT to provide operating units that do not have their own CIRT with an incident response capability. The DOC CIRT is also intended to serve as a focal point for disseminating best practices and incident response methodologies to all Commerce CIRTs.

The Department's information security policy defines the types of incidents that need to be reported, sets minimum requirements for incident response capabilities, and prescribes the system-level processes and incident-handling procedures to be performed, including reporting incidents to FedCIRC. It establishes requirements for monitoring and detecting incidents, including use of network- and host-based intrusion detection systems, logging tools, firewalls, and other devices, as well as review of audit logs, trouble reports, and information provided by intrusion detection tools. Finally, it requires each operating unit to submit its response procedures to Commerce's CIP program manager for review and approval—action that will ensure all units have documented procedures for reporting security incidents and sharing information about common vulnerabilities.

According to the policy, all DOC system users and system and network administrators are to report incidents to the operating unit's designated CIRT. The team, in turn, must complete an incident report and forward it to the DOC CIRT in a secure manner such as by encrypted transmission. Preliminary reporting must occur within 24 hours of the event's discovery, after which the CIRT has 5 working days to submit a complete and detailed report to the DOC CIRT. The policy requires operating unit CIRTs to report incidents to FedCIRC and send an informational copy of the report to the DOC CIRT. It makes the DOC CIRT responsible for reporting incidents to FedCIRC for those units that do not have their own response teams. However, it does not specify a timeframe within which FedCIRC must be notified.

[21] A patch is object code (code produced by a compiler) that is inserted into an executable program to temporarily fix a program error or security issue.

The MOA between OIG, CIO, and OSY further delineates roles, responsibilities, and procedures for reporting incidents to OIG and external law enforcement. To ensure these procedures are followed, they need to be incorporated into or referenced by the Department's information security policy after the new MOA is completed.

Configuration requirements

The Department's policy requires system owners to establish procedures for configuration management of all general support systems and major applications. System security plans must describe how changes to the system or application will be authorized, controlled, tested, and implemented. However, with the exception of certain specific requirements for perimeter security devices and firewalls contained in the information security policy, the Department has not developed specific configuration requirements or defined system security settings. Several of the operating units we reviewed—ITA, NIST, and NOAA—told us that they have provided configuration requirements for specific products based on NIST or National Security Agency (NSA) guidance.

The Department's policy requires each operating unit IT security officer to have a process and documented procedures in place to identify, track, and report on security patch management. It stipulates that operating units centralize patch management leadership so that timely attention is given to patches for all systems and duplication of patch management functions is minimized.

The operating units we assessed—Census, ITA, NIST, and NOAA—have manual patch management processes; however, most are seeking to automate at least some portions of the process.

FedCIRC provides the web-enabled Patch Authentication and Distribution Capability (PADC), a free, secure source of validated patches. PADC notifies users about new threats or vulnerabilities that could disrupt federal government systems and networks and provides patches that have been verified as secure and able to eliminate the intended vulnerability. This service is valuable because patches must otherwise be downloaded from Internet sites, some of which have been attacked by hackers who have corrupted the patches with malicious code. Commerce has access to PADC, but is just beginning to use it. According to the Department CIO, Commerce will rely on PADC for notification of threats and for tested patches.

USPTO

Incident Handling and Reporting

USPTO has draft incident response procedures, which it intends to finalize by the end of the fiscal year. The procedures are detailed and specific, but do not address a timeframe for reporting incidents to FedCIRC or notification of OIG when an incident occurs. The director of the IT Security Program Office told us that modifications will be made to address these omissions before the procedures are finalized.

Configuration requirements

USPTO officials told us that while the agency has configuration requirements, its certification activities found that the settings could not be traced to an authoritative source such as NIST or NSA. USPTO plans to implement the vendor recommended security settings.

USPTO has a patch management policy and procedures, has an automated tool to deploy patches and monitor their application, and is a PADC user. According to the director of the IT Security Program Office, IT personnel can view the status of patches on all servers and all but one operating system, and will soon be able to view the status of patches on that remaining system as well. However, certification testing found that appropriate security settings and patches are not always implemented. USPTO reports that five IT staff members are registered users of PADC.

Responsibilities of Program Officials and Chief Information Officers

Risk assessments, security level determinations, security plans, and security control testing and evaluation. (OMB Question C.1)

XI. The Department's Risk Assessments, Security Plans, and Testing of Security Controls Continue to Need Serious Attention

FISMA assigns senior agency officials and the CIO responsibility for assessing the information security risks for programs and systems over which they have control, determining the levels of information security appropriate to protect associated operations and assets, and periodically testing and evaluating information security controls and techniques. In turn, the Department's policy has charged all operating unit officials and CIOs with these same responsibilities in their organizations.

In last year's independent evaluation, we found numerous systems operating without required risk assessments or approved security plans. Some that had approved security plans provided no evidence that risk analysis—a prerequisite for the security plan—had been conducted. Most operational systems had not been certified and accredited, and those that were frequently lacked evidence that the requisite security testing and evaluation had been performed. As noted previously, the Department CIO set September 30, 2003, as the deadline for having all national-critical and mission-critical systems certified and accredited.

In June 2003, we requested certification and accreditation materials, including risk assessments, security plans, contingency plans, and security test and evaluation materials (test procedures and results) for a range of systems we selected throughout the Department. As shown in table 5, our review of these materials for 37 systems in 6 operating units (including 5 NOAA line offices) found serious deficiencies in the content and quality of the risk assessments and plans. We found many risk assessments and security plans that did not provide essential information for determining appropriate system security controls, and still others whose information was inaccurate or inconsistent. We also found that the certifications were frequently granted without careful review of the documentation and without testing, and thus did not identify residual risks.[22] Without reliable documentation and certifications, accrediting officials lack sufficient information for making informed decisions about whether a system's residual risks are acceptable and accreditation is therefore desirable. (Through accreditation, the DAA is explicitly accepting the residual risks; therefore, these risks must be clearly identified.)

In cases where testing was conducted, it was usually in the form of vulnerability scans,[23] which, while a useful part of the testing process and required annually by the Department's policy, do not adequately cover security controls for certification purposes for any but low-risk systems. Certification test and evaluation should include such measures as penetration testing, observation of how controls are implemented, document review, and interviews.

[22]Residual risks are the risks remaining after appropriate security controls have been applied to the information system.
[23]Vulnerability scans use automated tools to identify vulnerabilities of computing systems in a network in order to determine whether and where a system can be exploited or threatened.

The deficiencies we identified affected systems controlled by program officials as well as by operating unit CIOs. Details of our evaluation criteria and results for each operating unit that we assessed are presented in Appendix A. We recognize that a number of Commerce systems, including ones that we reviewed, are undergoing recertifications and reaccreditations, which are scheduled to be completed by September 30, to comply with the new information security policy. According to the Department CIO, improvements are being made as part of this process that should correct a number of the problems we identified with the current accreditations.

Table 5: Summary of OIG Evaluation of Commerce Certification and Accreditation Materials*

Criteria	OIG Evaluation
Number of systems reviewed	37
Number of systems certified and accredited	30
Number of systems certified and accredited with adequate testing	0
Number of systems certified and accredited with residual risks identified	0
Number of risk assessments that provide a sufficient basis for identifying security controls	11
Number of security plans that adequately:	
--Describe applications/data/data flow	7
--Identify interconnections	15
--Provide support for assigned sensitivity levels	9
Number of contingency plans that adequately:	
--Identify alternate sites	14
--Describe backup procedures	28
--Describe system restoration procedures	7

*Assessment covered systems in the following operating units: BEA, BIS, Census, NIST, NTIS, and NOAA (NESDIS, NMFS, NOS, NWS, and OAR).

Risk assessments, security level determinations, security plans, and security control testing and evaluation. (OMB Question C.1)

XII. USPTO Is Making Significant Improvements to Risk Assessments, Security Plans, and Testing of Security Controls

Based on the materials that we reviewed for USPTO's one certified and accredited system, it is evident that the agency has made an extremely conscientious effort to employ a disciplined process using the NIACAP standard. This system had a thorough risk assessment and comprehensive security and contingency plans. Certification included extensive testing of security controls that identified weaknesses in the system itself, as well as organization-wide security issues. We note, however, that the security plan only provided examples of interconnections with other systems, rather than identifying all interconnections, as directed by NIST guidance. Overall, USPTO has a sound approach, which it appears to be using for certifying and accrediting its remaining systems.

As we discussed previously, of the 10 systems scheduled to be certified and accredited this fiscal year, 1 has been fully accredited and 5 had been granted interim accreditations. USPTO expects the remaining 4 systems to receive interim accreditations by the September 30 deadline. The agency's interim accreditations require comprehensive risk assessments, security plans, and testing of security controls. As USPTO corrects the problems identified by means of its certification and accreditation process, its systems will be appreciably more secure.

XIII. The Department CIO Continues to Make Progress in Improving Information Security Throughout Commerce

The agency CIO's ability to adequately maintain an agencywide information security program, ensure effective implementation of the program, and evaluate the performance of major agency components. (OMB Question C.2)

Over the past several years, the Department CIO has focused intensely on improving information security and has made significant strides. In finalizing the new information security policy this past January, he gave Commerce a comprehensive blueprint for securing agency information systems that complies with the minimum requirements for security programs set forth in OMB Circular A-130: namely, that each system have (1) a knowledgeable Commerce official assigned responsibility for its security, (2) a risk assessment and security plan, (3) a periodic review of its security controls, and (4) authorization to operate (certification and accreditation). As required by FISMA, the CIO has designated a senior officer for information security.

The Department CIO is making a determined effort to effectively implement the security program, though much remains to be done—especially in the areas of assessing risk, determining appropriate security controls, testing and evaluating these controls, and certifying and accrediting systems. But satisfying the demands of information security law, policy, and guidance requires substantial change in the culture of an organization that, until recently, has given scant attention to this area. Thus, it remains a considerable challenge to ensure that program and IT officials throughout the Department understand and accept their information security responsibilities and that personnel with specialized information security roles continually increase their knowledge and skills to address a technically complex and constantly changing security environment.

The Department CIO's Office has initiated a compliance review program to evaluate the performance of all Commerce operating units by validating the security information they report and assessing the effectiveness of their information security programs. As noted previously, the CIO intends to review all systems over a 3-year cycle. The fiscal year 2003 review has three objectives: (1) validate the system inventory, (2) inspect the quality of certification and accreditation packages for all classified, national-critical, and mission-critical systems in the inventory as of March 2003, and (3) verify implementation of corrective actions to resolve the recommendations from GAO reports issued in August 2001 and January 2002. The Department CIO Office's management and oversight of the POA&M process is an additional means by which it evaluates operating unit performance.

USPTO

Last fiscal year, USPTO's newly appointed CIO began giving serious attention to improving information security and establishing and maintaining an agencywide information security program, and excellent progress has been made as a result. USPTO's information security policies, when refined and finalized, should address the basic security program requirements of OMB Circular A-130 that each system have a knowledgeable USPTO official assigned

responsibility for its security, a risk assessment and security plan, a periodic review of its security controls, and certification and accreditation. As required by FISMA, a senior agency information security officer has been designated by USPTO's CIO. And as we have discussed previously, USPTO is well on its way to certifying and accrediting all of its mission-critical systems and is using sound processes to do so.

Like the rest of the Department, effectively implementing the stipulated information security program requires significant cultural change. USPTO's CIO is currently working with program officials to facilitate their understanding and acceptance of their more active role and increased accountability before the policy is finalized. We believe that the CIO's effort is essential to initiating and maintaining an efficacious information security program.

The ongoing certification and accreditation efforts, the POA&M process, and the work of the internal IT auditor (i.e., unannounced penetration testing of networks and systems and review of security documentation) are the principal means by which its major components are currently being evaluated. The Department intends to assess USPTO as part of its compliance review, which will provide an additional means of evaluation.

The agency CIO's efforts to ensure that all agency employees, including contractors and those employees with significant information security responsibilities, are aware of and trained in information security policies and practices. (OMB Question C.3)

XIV. Information Security Awareness Training Is Being Addressed, but Specialized Training Requirements Are Needed

The Department's new policy requires each operating unit's information security program to include an awareness, training, and education component for all employees and contractors, remote researchers and collaborators working on Commerce projects, and temporary guest system users. New employees and contractors must receive awareness training within 30 days of hire and prior to using any IT resource. All existing employees and contractors who have access to systems containing sensitive information are required to have annual refresher training. Operating units must maintain a tracking system that identifies those trained, and the type and date of training taken.

Department and operating unit officials told us that security awareness training is provided annually for all employees and contractor personnel. During this fiscal year, the CIO enhanced and disseminated its awareness training for new employees and acquired an enterprise license for web-based information security training, which has recently made awareness refresher training customized for Commerce available at no charge to Commerce employees and contractors. This training is provided by the Gov Online Learning Center (referred to as GOLearn).[24]

Specialized training. Under the Department's policy, operating units must identify positions that require specialized training as well as the specific requirements of that training. We found limited progress in this area. Training for personnel with significant information security responsibilities, such as system administrators, IT security officers, and contracting officers, appeared to be inconsistent and incomplete at the units we reviewed. The Department has been attempting to establish more uniform requirements or guidance for specialized training, but progress here has been slow. A working group convened in FY 2001 to address specialized training helped develop the Department's training policy and conducted a needs assessment, but has not defined requirements for specialized training. In the meantime, the Department CIO is making training more accessible: the recently acquired enterprise license will make specialized training available throughout Commerce at a nominal cost. The approximately 60 GOLearn courses are mapped to various positions identified in NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* One area that is progressing is training of procurement personnel. As discussed in Finding I, OAM has developed security training for these personnel, which is undergoing review.

In conducting our independent evaluation this year, we found that some IT security officers and system administrators still do not sufficiently understand their duties and responsibilities. We also found a pervasive lack of understanding of the objectives and requirements of system risk

[24] The Gov Online Learning Center offers web-based training to federal employees.

assessment, security planning, contingency planning, and certification and accreditation. These findings highlight the importance of ensuring that specialized security training is provided to those who need it.

USPTO

USPTO is using GOLearn through the Department's enterprise license to provide the mandated annual awareness refresher training in information security awareness, and also requires awareness training for new employees and contractors. USPTO has not yet established requirements for specialized training and is using NIST training guidance to do so. In the meantime, USPTO executives have received specialized training in information security, including certification and accreditation, and CIO managers and staff have been trained on USPTO's IT processes and related information security procedures, as have some program, administrative, and contractor employees. USPTO plans to implement specialized training for approximately 150 employees and contractors, also via GOLearn. As noted, these courses are mapped to various positions identified in NIST guidance.

XV. Integration of Security into the Capital Planning and Investment Control Process Is Improving

Agency CIO's efforts to fully integrate security into the capital planning and investment control process. (OMB Question C.4)

Our review of capital asset plans last year revealed that the operating units need to do a better job of identifying security risks and controls in their capital asset plan so as to improve and better justify projections of security expenditures. This year, we reviewed FY 2004 plans for BIS, NESDIS, NOS, NWS, and NTIA (FY 2005 plans were not available when we conducted our fieldwork) and noted that in general, they contained more specific information on security requirements and how they are addressed. Some, however, still contained generic discussions of security requirements and controls, and one plan was ambiguous about whether the system had been certified and accredited. All of the plans stated that the system's security controls had been tested, but few described the test methodology. Our review of security materials, as noted in Finding XI, found little if any testing of security controls for most systems beyond self assessments.

USPTO

We reported last year that USPTO had not identified security costs for any individual system in its FY 2002 or FY 2003 budget submissions. In this year's review, we found that capital asset plans prepared for the FY 2004 submission comprehensively addressed the areas required by OMB and thus demonstrate a serious effort by USPTO to include information security in its capital asset planning.

XVI. Conclusion

Our FY 2003 FISMA review found that senior management continues to give attention and priority to information security. With the support of the Deputy Secretary, the Department's CIO has worked hard to improve information security throughout Commerce. In January 2003, the CIO finalized a new information security policy that comprehensively defines Commerce's program for protecting agency information systems, and its detailed requirements are helping improve the security programs of the operating units. Responsibilities are clearly delineated for Commerce's senior agency officials and CIOs, system life-cycle information security requirements are specified, and security is becoming better integrated into the capital planning and investment control process.

This noteworthy progress is moderated by the considerable challenges that persist, the greatest of which is ensuring adequate security on the hundreds of Commerce systems. Much remains to be done in this regard, especially in assessing risk and determining appropriate security controls, testing and evaluating these controls, certifying and accrediting systems, and ensuring that personnel with specialized information security responsibilities receive the necessary training. As we have pointed out previously, implementing an effective information security program throughout Commerce requires both education and substantial cultural change. Until program and IT officials throughout the Department better understand what is expected of them, and all personnel with specialized information security roles acquire and maintain the requisite knowledge and skills, the security of many Commerce systems remain problematic.

USPTO

USPTO's information security program continues to progress. This agency is working to ensure that its senior program officials understand and accept their responsibilities for information security, a prerequisite for an effective and long-lived program. Security has become better integrated into the capital planning and investment control process for IT, and system life-cycle information security requirements and processes are being improved. Significantly, USPTO is well on its way to having its systems certified and accredited. And because it is using a rigorous approach and comprehensive testing, it has gained a great deal of insight into system-specific weaknesses that must be corrected and organization-wide security policies, procedures, and processes that must be improved. USPTO must continue to focus on actions to correct the identified system weaknesses; improve policies, procedures and processes; and ensure compliance on a continuing basis.

Appendix A. Evaluation of Certification and Accreditation Materials

In answer to OMB Question C.1, this appendix presents the results of our evaluation of the extent to which operating unit program officials and CIOs have—for the systems for which they are responsible—(1) assessed risks, (2) determined appropriate security levels, (3) maintained security plans, and (4) tested and evaluated security controls. We reviewed the following information for 37 systems in 6 operating units, including 5 NOAA line offices:[25]

- Risk assessment
- Security plan
- Contingency plan
- Security test and evaluation materials (test procedures and results)
- Any additional certification and accreditation materials
- Any reports that document an independent security assessment of the system (e.g., a contractor assessment)

In reviewing this information, we focused on whether the following had been accomplished:

Systems have been certified and accredited with adequate testing. Testing security controls is essential for validating that the required controls are in place and working as intended, and is a key part of system certification.

Residual risks have been identified for certified and accredited systems. Residual risks are the risks remaining after appropriate security controls have been incorporated in a system. In accrediting a system, the DAA is explicitly accepting the residual risks; therefore, these risks must be clearly identified.

Risk assessments provide a sufficient basis for identifying security controls. To determine system security controls that appropriately balance the cost of protective measures against operational and economic costs, risks must be identified and their impacts assessed.

Security plans adequately describe applications, data, data flow, and system interconnections, and support the assigned sensitivity levels. This is fundamental information for planning system security. Sensitivity levels are determined to be low, medium, or high based on requirements for confidentiality, integrity, and availability of the information handled, and are needed to design appropriate security controls.

Contingency plans identify alternate processing sites, and describe system backup and restoration procedures. This is basic information to enable the recovery of systems, operations, and data after a disruption.

We were able to determine whether a system's risk assessment, security plan, or contingency plan generally provided the appropriate information, but without a thorough assessment of the system

[25] Our evaluation of USPTO is presented separately in Finding XI.

itself, we could not determine whether the information was complete or wholly accurate. In many cases, however, information was clearly missing, inconsistent with other information presented, or not responsive to the intent of the document. Although some operating units sent us draft materials, we evaluated final documentation only.

We present our findings for the operating units we reviewed in the tables below, showing for each the number of evaluated systems that met the corresponding OMB criterion. Where additional information is useful, we include brief comment.

Table A-1: Bureau of Economic Analysis

Criteria	OIG Evaluation	
Number of systems reviewed	3	
Number of systems certified and accredited	2	
Number of systems certified and accredited with adequate testing	0	
Number of systems certified and accredited with residual risks identified	0	
Number of risk assessments that provide a sufficient basis for identifying security controls	1	
Number of security plans that adequately:		
--Describe applications/data/data flow	1	
--Identify interconnections	3	
--Provide support for assigned sensitivity levels	2	One plan had assigned medium confidentiality to publicly available information.
Number of contingency plans that adequately:		One plan covered all 3 systems (the local area network and 2 applications), and contained detailed procedures and evidence of recent testing.
--Identify alternate sites	3	
--Describe backup procedures	3	
--Describe system restoration procedures	3	

Table A-2: Bureau of Industry and Security

Criteria	OIG Evaluation	
Number of systems reviewed	3	
Number of systems certified and accredited	0	Two systems have interim accreditations that expire in late September 2003. For 1 system, no documentation was provided to support the 12/31/02 accreditation.
Number of systems certified and accredited with adequate testing	0	Automated vulnerability scan results were provided for 1 system.
Number of systems certified and accredited with residual risks identified	0	
Number of risk assessments that provide a sufficient basis for identifying security controls	1	
Number of security plans that adequately:		
--Describe applications/data/data flow	1	
--Identify interconnections	2	
--Provide support for assigned sensitivity levels	1	
Number of contingency plans that adequately:		
--Identify alternate sites	0	
--Describe backup procedures	1	
--Describe system restoration procedures	0	

Table A-3: Census Bureau

Criteria	OIG Evaluation	
Number of systems reviewed	4*	
Number of systems certified and accredited	4	
Number of systems certified and accredited with adequate testing	0	
Number of systems certified and accredited with residual risks identified	0	
Number of risk assessments that provide a sufficient basis for identifying security controls	1	
Number of security plans that adequately:		
--Describe applications/data/data flow	2	
--Identify interconnections	4	
--Provide support for assigned sensitivity levels	3	
Number of contingency plans that adequately:		
--Identify alternate sites	3	
--Describe backup procedures	3	
--Describe system restoration procedures	2	

*We reviewed general support systems for the National Processing Center and Geography division. The Geography system has four components, three of which had final documentation. Documentation for the fourth is being developed. We assessed the three that have final documentation, treating them as separate systems for purposes of this review. Census plans to accredit the fourth component and the Geography system as a whole in early FY 2004.

Table A-4: National Institute of Standards and Technology

Criteria	OIG Evaluation	
Number of systems reviewed	5	
Number of systems certified and accredited	5	IT security officer is reviewing all certified and accredited systems and making recommendations for improvement. Vulnerability scans are being required as a condition of staying on the network.
Number of systems certified and accredited with adequate testing	0	
Number of systems certified and accredited with residual risks identified	0	
Number of risk assessments that provide a sufficient basis for identifying security controls	2	
Number of security plans that adequately:		
--Describe applications/data/data flow	1	
--Identify interconnections	2	
--Provide support for assigned sensitivity levels	0	Two systems did not address sensitivity, and the remaining 3 did not justify the sensitivity levels assigned.
Number of contingency plans that adequately:		Two systems had no contingency plan.
--Identify alternate sites	1	
--Describe backup procedures	3	
--Describe system restoration procedures	2	

Table A-5: National Technical Information Service

Criteria	OIG Evaluation	
Number of systems reviewed	3	
Number of systems certified and accredited	0	All 3 systems have expired interim accreditations. NTIS plans to reaccredit these systems by end of the fiscal year.
Number of systems certified and accredited with adequate testing	0	Interim accreditation letters state that testing was performed, but no evidence was provided.
Number of systems certified and accredited with residual risks identified	0	Interim accreditation letters state that residual risks were considered, but none were identified. Vulnerability scans were conducted after interim accreditation was granted.
Number of risk assessments that provide a sufficient basis for identifying security controls	0	No risk assessments were provided.
Number of security plans that adequately:		
--Describe applications/data/data flow	0	
--Identify interconnections	0	
--Provide support for assigned sensitivity levels	0	
Number of contingency plans that adequately:		
--Identify alternate sites	0	
--Describe backup procedures	3	
--Describe system restoration procedures	0	

Table A-6: NOAA-National Environmental Satellite, Data, and Information Service

Criteria	OIG Evaluation	
Number of systems reviewed	3	Two of the systems were evaluated as part of our FY 03 in-depth FISMA reviews.
Number of systems certified and accredited	3	
Number of systems certified and accredited with adequate testing	0	
Number systems certified and accredited with residual risks identified	0	
Number of risk assessments that provide a sufficient basis for identifying security controls	0	Risk assessments were hazard matrices, which do not provide a sufficient basis for determining controls.
Number of security plans that adequately:		
--Describe applications/data/data flow	0	
--Identify interconnections	0	
--Provide support for assigned sensitivity levels	1	
Number of contingency plans that adequately:		
--Identify alternate sites	1	
--Describe backup procedures	3	
--Describe system restoration procedures	0	

Table A-7: NOAA-National Marine Fisheries Service

Criteria	OIG Evaluation	
Number of systems reviewed	2	Both systems were evaluated as part of our FY 03 in-depth FISMA reviews.
Number of systems certified and accredited	2	
Number of systems certified and accredited with adequate testing	0	
Number systems certified and accredited with residual risks identified	0	
Number of risk assessments that provide a sufficient basis for identifying security controls	2	Risk assessments did not use NOAA's standard hazard matrices and were more complete.
Number of security plans that adequately:		
--Describe applications/data/data flow	0	
--Identify interconnections	0	
--Provide support for assigned sensitivity levels	0	
Number of contingency plans that adequately:		
--Identify alternate sites	1	
--Describe backup procedures	2	
--Describe system restoration procedures	0	

Table A-8: NOAA-National Ocean Service

Criteria	OIG Evaluation	
Number of systems reviewed	3	
Number of systems certified and accredited	3	
Number of systems certified and accredited with adequate testing	0	Vulnerability scans performed on 2 systems; password strength tested on 1 system.
Number systems certified and accredited with residual risks identified	0	
Number of risk assessments that provide a sufficient basis for identifying security controls	0	Risk assessments were hazard matrices, which do not provide a sufficient basis for determining controls.
Number of security plans that adequately:		
--Describe applications/data/data flow	1	
--Identify interconnections	3	The list of interconnections in one plan may not be complete, because some that are cited elsewhere in the plan are not on the list.
--Provide support for assigned sensitivity levels	1	Confidentiality not well supported in 2 plans, and both had conflicting confidentiality levels.
Number of contingency plans that adequately:		
--Identify alternate sites	0	Contingency plans address the need to establish alternate sites, but do not identify the sites.
--Describe backup procedures	3	
--Describe system restoration procedures	0	

Table A-9: NOAA-National Weather Service

Criteria	OIG Evaluation	
Number of systems reviewed	7	
Number of systems certified and accredited	7	
Number of systems certified and accredited with adequate testing	0	
Number systems certified and accredited with residual risks identified	0	
Number of risk assessments that provide a sufficient basis for identifying security controls	0	Risk assessments were hazard matrices, which do not provide a sufficient basis for determining controls.
Number of security plans that adequately:		
--Describe applications/data/data flow	1	
--Identify interconnections	1	
--Provide support for assigned sensitivity levels	0	One system's confidentiality level was based on an inaccurate description of the data, while the remaining systems did not support assigned sensitivity levels.
Number of contingency plans that adequately:		
--Identify alternate sites	7*	
--Describe backup procedures	3	
--Describe system restoration procedures	0	

*Three systems are covered in contingency plans for site certifications and accreditations.

Table A-10: NOAA-Office of Atmospheric Research

Criteria	OIG Evaluation	
Number of systems reviewed	4	
Number of systems certified and accredited	4	
Number of systems certified and accredited with adequate testing	0	OAR stated that these systems do not require testing beyond NIST self-assessment; however, based on their sensitivity, we believe thorough testing is required.
Number of systems certified and accredited with residual risks identified	0	
Number of risk assessments that provide a sufficient basis for identifying security controls	4	OAR augmented NOAA's standard hazard matrices with more complete risk assessments.
Number of security plans that adequately:		
--Describe applications/data/data flow	0	
--Identify interconnections	1	
--Provide support for assigned sensitivity levels	1	One system indicated that it carries Privacy Act, financial, and credit card information; however, the system is a meteorological system used to obtain scientific atmospheric information. This inaccuracy appears to have resulted from sections being cut and pasted from another plan without sufficient revision.
Number of contingency plans that adequately:		One plan (for a different system than that cited above) had sections cut and pasted from another plan without sufficient revision (e.g., the wrong system is cited in places).
--Identify alternate sites	1	
--Describe backup procedures	4	
--Describe system restoration procedures	0	

Appendix B. OIG Evaluations Used In This Report

1. National Oceanic and Atmospheric Administration, *Stronger Security Controls Needed to Protect NMFS Information Technology Systems,* Inspection Report No. OSE-15693, September 2003.

2. National Oceanic and Atmospheric Administration, *Stronger Security Controls Needed to Protect NESDIS' Headquarters Local Area Network,* Inspection Report No. OSE-15996-3-0001, September 2003.

3. National Oceanic and Atmospheric Administration, *Stronger Security Controls Needed to Protect NESDIS Research Data System*, Inspection Report No. OSE-15996-3-0002, September 2003.

4. Office of the Secretary, *Review of IT Controls to Support the FY 2002 Consolidated Financial Statement Audit,* Audit Report No. FSD-15214-3-0001, January 2003.

5. National Technical Information Service, *Improvements Needed in the General Controls Associated with NTIS's Financial Management Systems*, Audit Report No. FSD-15212, December 2002.

6. United States Patent and Trademark Office, *Improvements Needed in the General Controls Associated with USPTO's Financial Management Systems*, Audit Report No. FSD-15213, December 2002.