U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

OFFICE OF THE SECRETARY

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

Executive Summary

Final Inspection Report No. OSE-15260/September 2002

PUBLIC
RELEASE

Office of Systems Evaluation

TABLE OF CONTENTS

INTRODUCTION

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

GISRA requires (1) annual agency program reviews, (2) annual independent OIG evaluations, (3) agency reporting of the results of the OIG evaluations to the Office of Management and Budget (OMB), and (4) an annual OMB report to Congress summarizing the agency materials received. In accordance with OMB guidance, agency heads are to transmit to OMB both the OIG's independent evaluation and the agency's program review.[1]

OBJECTIVES, SCOPE, AND METHODOLOGY

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

- National Institute of Standards and Technology, *Additional Improvements Needed to Strengthen NIST's Information Security Program,* Inspection Report No. OSE-15078/September 2002.

- Office of the Secretary, *Information Security Requirements Need to Be Included in the Department's Information Technology Service Contracts,* Inspection Report No. OSE-14788/May 2002.

- U.S. Department of Commerce, *Consolidated Financial Statements, Fiscal Year 2001, Improvements Needed in the General Controls Associated with the Department's Financial Management Systems,* Audit Report No. FSD-14474-2-0001/February 2002.

- Bureau of the Census, *Improvements Needed in the General Controls Associated with Census' Financial Management Systems,* Audit Report No. FSD-14473-2-0001/February 2002.

[1] As a performance-based organization, the United States Patent and Trademark Office (USPTO) submits its information security review separate from that of the Department of Commerce. For FY01, we submitted the same independent evaluation for USPTO as for the Department because our evaluation addressed the status and issues associated with the Department as a whole, including USPTO. However, because USPTO is undertaking actions separate from the Department's to manage information security, we have reviewed and reported on USPTO's information security program separately this year.

- National Technical Information Service, *Improvements Needed in the General Controls Associated with NTIS's Financial Management Systems*, FSD-14476-2-0001/February 2002.

- National Oceanic and Atmospheric Administration, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-14475-2-0001/February 2002.

To obtain additional information regarding the responsibilities of the agency head, training of personnel with significant information security responsibilities, and integration of information security into the capital planning and investment control process, we interviewed or received written materials from the chief information officers (CIOs) and senior information security officials of the Department and the following operating units: Bureau of Industry and Security (BIS), International Trade Administration (ITA), National Telecommunications and Information Administration (NTIA), and National Oceanic and Atmospheric Administration (NOAA). We also requested that these units provide the risk assessment, security plan, security testing and evaluation materials (test procedures and results), and certification and accreditation[2] documents for the systems shown in Table 1.

We conducted our evaluation using the following criteria: NIST's *Security Self-Assessment Guide for Information Technology Systems*, GISRA, the Computer Security Act, OMB Circular A-130, "Management of Federal Information," and NIST guidance on conducting risk assessments and preparing information security plans. OIG contractors conducted the general control reviews of financial systems, using GAO's *Federal Information System Controls Audit Manual* (FISCAM) as a guide.

The structure and content of this report respond to guidance provided by OMB in *Reporting on the Government Information Security Reform Act.* 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.

[2] 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.

Table 1. Additional Operating Units/Systems Assessed

Bureau of Industry and Security (BIS)
Export Control Automated Support System
Communication Infrastructure
Chemical Weapons Convention Information Management System
BXA/NEC Technical Information Center Training Local Area Network (LAN)
International Trade Administration (ITA)
Headquarters Network
Field Network
Trade Policy Information System
Web Presence
National Telecommunications and Information Administration (NTIA)
Grant Application Monitoring and Processing System
LAN
National Oceanic and Atmospheric Administration (NOAA)
Office of Oceanic and Atmospheric Research (OAR)
Headquarters Administrative Computing Facility
Atlantic Oceanographic and Meteorological Laboratory
Forecast Systems Laboratory Central Facility
Geophysical Fluid Dynamics Laboratory Scientific Computing Facility
National Severe Storms Laboratory Scientific Computing Facility
Space Environment Center Space Weather Operations

National Oceanic and Atmospheric Administration (NOAA) (continued)
National Ocean Service (NOS)
LAN Backbone System
National Water Level Observation Data Management System Network
Geodetic Support System
Physical Oceanographic Real-Time System (PORTS)
Remote Sensing System
National Environmental Satellite Data and Information Service (NESDIS)
Central Environmental Satellite Computer System
National Geophysical Data Center Data Archive Management and User System
National Climatic Data Center (NCDC) Ingest and Processing Computing and Communications System
Research Data Systems
NCDC Archive
NCDC Local Area Network
Satellite Operations Control Center-Geostationary Orbiting Environmental Satellite Ground System
National Marine Fisheries Service (NMFS)
Headquarters Wide Area Network
Vessel and Logbook Management
Woods Hole Facility LAN
Mississippi Laboratories and Stennis Space Center LAN
Northwest Fisheries Science Center LAN
Honolulu Laboratory LAN

FINDINGS

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

GISRA requires that significant deficiencies in security policy, procedures, or practices be reported as material weaknesses. OMB Circular A-130 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. As discussed in this report, the Department has made significant progress over the past year in establishing the foundation for an effective information security program. However, much remains to be done, given the severity of Commerce's information security weaknesses and the magnitude and complexity of the effort needed to address them. Consequently, this area continues to be an OIG top 10 management challenge.

Commerce has established September 30, 2002, as the deadline for having approved security plans for all operational systems. In the operating units we evaluated, 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 have not been accredited, and those that are accredited frequently lack evidence that the requisite security testing and evaluation have been performed, thus diminishing the assurance that accreditation is intended to impart. When implemented properly, accreditation is a powerful method for helping assure that effective management, operational, and technical controls are in place and functioning as intended. The Department recognizes the importance of certification and accreditation, as well as the need for management and information security personnel throughout Commerce to better understand the objectives and requirements of these processes, and has recently provided training for the operating units.

We believe that in the coming year, the Department should focus on ensuring that all operational systems have approved security plans of adequate content and quality and that these systems undergo rigorous certification and accreditation processes. The Department reported information security as a management control (material) weakness in its FY01 Accountability Report; we believe it should continue to be reported as such until all of the Department's national-critical[3] and mission-critical systems are accredited.

II. Department Senior Management Officials Have Made a Commitment to Improving Information Security

Improving information security remains a priority for the Department. Its importance has been emphasized to senior management by the Secretary and Deputy Secretary of Commerce, resulting in senior management officials in the operating units increasing their attention to this area, as well. The Department CIO must concur with all decisions to invest in major information technology (IT) systems or projects,[4] and therefore can ensure that adequate security is planned for these systems. A Project Matrix review is being conducted, which is an assessment that will identify the Department's critical assets and any public or private systems on which they depend.

A. Senior Management Officials Are Taking Action to Support Information Security Improvements

We reported in last year's independent evaluation that the Department was making a concerted effort to improve information security and make it an integral component of Commerce's business operations. The Department had taken two important steps toward achieving these goals: Specifically, the Secretary of Commerce directed secretarial officers and heads of operating units to (1) give information security high priority, sufficient resources, and their personal attention, and (2) restructure (and thus strengthen) IT management by having a CIO at

[3] National critical systems are part of the nation's critical infrastructure.

[4] A major IT system or project is a system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

each unit who reports to the unit head or principal deputy and to the Department CIO, and by increasing the unit CIO's authority over IT resources. We noted that these actions—if accompanied by continued executive-level attention and adequate resources—are important steps in building a more effective information security program.

Our evaluation this year confirmed that Department-level executive support for information security continues. At departmental Executive Management Team meetings with senior Commerce officials, both the Secretary and Deputy Secretary reportedly have emphasized the importance of information security, stating that a lack of resources (financial or otherwise) is not an acceptable reason for failure to improve. Moreover, the Deputy Secretary has reinforced senior management's responsibility for establishing effective information security programs in the operating units and for correcting the problems identified by OIG and GAO evaluations.

As discussed below, our review of selected operating units found that senior management officials generally are giving information security their personal attention and are working to ensure that employees understand the responsibilities of their unit's CIO and program officials.

Senior management in BIS, ITA, and NOAA, for example, have supported efforts to ensure that the Department CIO's information security guidance is implemented as it becomes available, and have incorporated an information security element in the performance plans of their CIOs and other unit personnel with IT responsibilities. BIS and ITA officials told us that the Under Secretaries discuss information security at their weekly staff meeting, where they receive a status report on the progress of the agencies' corrective action plans from their respective CIOs. BIS reallocated $500,000 to information security in FY02, while ITA devoted $372,000 in FY01 carryover funds to this issue. We were also told that at BIS, the Under Secretary and Deputy Under Secretary have requested briefings from their CIO on GISRA requirements, as well as on certification and accreditation, and the Deputy Under Secretary was given approving authority for system accreditation, an action that demonstrates a high level of commitment to assuring the security of BIS' sensitive systems and information.

According to NOAA officials, the Under Secretary for Oceans and Atmosphere has been briefed on information security issues, promoted security awareness training for all NOAA employees and contractors, and supported the realignment of information security resources in the line offices to allow for a full-time security officer in each office. NOAA officials also told us that the Under Secretary receives updates from NOAA's CIO on the status of the information security program at weekly staff meetings.

Because NTIA is a small unit (approximately 200 employees), the Assistant Secretary uses day to day communications with staff to ensure they understand information security responsibilities and implement required procedures. NTIA officials told us that the unit had information security directives in place and routinely followed related procedures prior to GISRA.

At NIST we found that, until recently, information security had not received adequate attention. Since May, however, when our fieldwork in this operating unit was completed, the director of NIST has taken important steps toward improving the information security program. In June, the director issued a memorandum acknowledging his responsibility for the security of NIST's data and IT systems. This memorandum directed all members of NIST's senior management to give information security high priority and to ensure that NIST's policies, procedures, and operational environment are exemplary. The director issued another memorandum to senior managers in September discussing the findings and recommendations of the OIG's information security evaluation and emphasizing his personal responsibility as director and their responsibility as program managers for good information security. The memorandum concluded by pointing out the importance of all employees understanding their responsibilities for information security, underscoring the need for NIST management to lead and promulgate improvements, and reaffirming the goal of making NIST an exemplary agency in securing its IT resources.

B. Most IT Investments Require CIO Concurrence

The Department CIO must concur with IT investment decisions for all major systems, and—with the exception of NIST—all of the operating units we reviewed require unit CIO concurrence for the remaining IT investments. By thus controlling IT spending decisions, the Department and operating unit CIOs can ensure that security is planned at the earliest stages of a system's life cycle.

At the Department level, the Commerce Information Technology Review Board,[5] chaired by the CIO, was established to support this decision-making function. The Department CIO, with input from the board, provides recommendations to the Secretary and Deputy Secretary through the Office of Budget on whether a proposed IT project should be funded. The board seeks to conduct a status review, usually once a year, for approved projects, and the CIO, in turn, uses these reviews to recommend whether a project should be continued, modified, or terminated. IT projects of more than $10 million that require a contract, as well as selected smaller projects, must be reviewed by the board for the acquiring operating unit to receive a delegation of procurement authority (authority to make contractual commitments). In his FY04 budget guidance to the operating unit CIOs, the Department CIO emphasized that demonstrating effective information security will be an important factor in the board's review of budget requests.

At the operating unit level, each CIO should review and concur with IT investments that are not subject to departmental approval, and Commerce policy requires units to have an IT capital planning and investment control process to accomplish the review process. At ITA and NTIA, the CIO must approve all IT investments. At BIS, all IT investments must be approved by a steering committee, of which the CIO is a member, and at NOAA, the CIO is a member of NOAA's IT investment review board, which must approve all investments exceeding $2.5 million. In the event the BIS or NOAA CIO does not concur with a proposed IT investment, the head of the operating unit is the deciding official. Because NIST just began to implement an IT capital planning and investment control process this fiscal year, investment decisions can be

[5] Other board members include the Chief Financial Officer and Assistant Secretary for Administration; Director, Office of Policy and Strategic Planning, Deputy CIO; the CIOs from NOAA, Census Bureau, NIST, ITA, and on a rotating term basis not to exceed two years, two other operating unit CIOs; selected operating unit executives as designated by the CIO; Director for Budget; Director for Acquisition Management, and Director for Human Resources Management.

made without the review and concurrence of NIST's acting CIO. NIST's response to our draft report noted that its capital investment planning process will be fully implemented in FY03.

C. Information Security, Critical Infrastructure, and Other Security Functions Appear Well Integrated

Both the Department's information security and critical infrastructure protection (CIP) programs are under the authority of the Department CIO. Systems considered national critical have priority in reviews performed by the CIO's office, which also coordinates with the Department's Office of Security to ensure that information security is addressed in its planning for continuity of operations. As we reported in last year's evaluation, in June 2001, the CIO's Office, Office of Security, and OIG entered into a memorandum of agreement to define their respective roles and responsibilities relating to the development, implementation, and management of the Commerce information security program. This agreement is intended to promote a partnership among the three offices that both ensures complete coverage of information security matters and prevents wasteful duplication of effort.

D. The Department's Critical Assets Are Being Identified

We reported last year that the reliability of the Department's asset inventory for the CIP program was questionable because of weaknesses in the methodology used to gather asset data; consequently, three of the Department's largest operating units expressed concern that the inventory did not reflect the priority of their assets. More recently, the federal Critical Infrastructure Assurance Office (CIAO) developed Project Matrix—a methodology for identifying critical assets that considers how quickly the asset would have to be reconstituted in an emergency.

Project Matrix uses a three-step process in which each civilian federal department and agency identifies (1) its critical assets, (2) other public sector assets on which those critical assets depend to operate, and (3) all associated dependencies on privately owned and operated critical infrastructures. The CIAO, in conjunction with the Department, pilot tested the methodology on three critical departmental assets, and in March, began a Project Matrix review of the entire Department. The first step of the Department-wide review (critical asset identification and prioritization) is currently concluding, and the CIAO has tentatively identified 42 assets as critical—1 each at NTIA, NIST, and Bureau of Economic Analysis (BEA), 3 at the Census Bureau, and the remaining 36 at NOAA. CIAO officials told us that they expect to have a draft report detailing these results by the end of October, but could not estimate when the second step—the public sector dependency analysis—would be completed.

III. Incident Response Reporting and Handling Procedures Are Being Improved

GISRA requires agencies to have documented procedures for detecting, reporting, and responding to information security incidents. In last year's evaluation, we found that only 4 of 15 operating units had a formal incident response capability and that the Department's policy for reporting information security incidents needed to be revised to specify OIG notification and to define what constitutes a reportable incident. In FY02, the Department established a computer incident response team (CIRT) to provide operating units that do not have their own CIRT with an incident response capability, thus ensuring coverage of the entire Department, and to be a focal point for obtaining and exchanging best practices and incident response methodologies. The Department CIO's office is also finalizing its draft information security program policy, which includes guidance on incident identification, handling, response, and reporting. According to the draft policy, Commerce's critical infrastructure program manager and IT security program manager, both located in the Department CIO's office, must approve all policies and procedures for operating unit incident response capabilities, thereby ensuring that all units have documented procedures for reporting security incidents and sharing information about common vulnerabilities. The draft policy sets minimum requirements for the units' incident response capabilities and prescribes the system-level processes and incident-handling procedures to be performed, including working with OIG investigators and other law enforcement authorities.

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

GISRA assigns senior agency officials 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 Secretary of Commerce has charged all operating unit heads with these same responsibilities for their organizations. GISRA also requires the Department's CIO to assist other senior officials with their information security responsibilities and to ensure that effective policies and procedures are implemented for the systems that support the CIO's functions. Operating unit CIOs are expected to perform the same function in their organizations.

The importance given to information security by Department senior management has increased the operating units' focus on these responsibilities during this past year, but significant shortcomings still exist. As noted earlier, the Department CIO set September 30, 2002, as the deadline for having approved security plans for all general support systems and major applications. A risk assessment, which determines the degree of an organization's exposure to security threats and identifies controls to counter risk, is a prerequisite for the security plan. However, as of July 2002—when our fieldwork concluded—we found a pervasive lack of risk assessments among the operating units, as well as numerous systems operating without approved security plans or accreditation. We found documentation of security control testing for only one system—a NOAA system at OAR. These deficiencies affected systems controlled by program officials as well as by operating unit CIOs. Our findings for the units we examined as part of this review are summarized below.

Operating Unit Findings

BIS. A risk assessment was provided for only one of the four systems for which we requested documentation, but security plans were provided for all four, and these were generally consistent with NIST guidance for content and format. Although BIS considers the plans approved, it lacks a formal approval process and thus could not validate the approval. None of the systems has undergone security testing and evaluation or been certified or accredited. However, BIS has developed a certification and accreditation policy based on the National Information Assurance Certification and Accreditation Process (NIACAP) and indicated that certification and accreditation will be completed for one system in September 2002 and for the remaining three systems by June 2003.

ITA. Risk assessments have been performed on the four ITA systems for which we requested documentation. ITA provided two security plans that it considers approved and two draft plans. However, like BIS, ITA lacks a formal approval process. Our review of the two approved plans found them to be generally consistent with NIST guidance for content and format, but in need of additional information regarding rules of behavior. Although these plans were developed after the Department released its new password policy, they do not comply with it. No systems have undergone security testing and evaluation or been certified or accredited.

Despite these issues, ITA is clearly making an effort to improve information security. It engaged a contractor to assess its information security program, infrastructure, and major applications. The contractor identified numerous serious weaknesses and recommended actions that, if taken, will significantly improve information security at ITA. The contractor's report noted that although ITA has not established a certification and accreditation process, the operating unit recognizes the importance of this process and is seeking best practices that it can follow.

NIST. At the time of our evaluation, none of NIST's 109 operational systems had a documented risk assessment or an approved security plan. Moreover, all but two lacked accreditation. NIST had established an ambitious schedule for accrediting all systems by September 1—a goal that required completed risk assessments, security plans, contingency plans, security testing and evaluation, and certification before that date. While we concurred that these important activities needed to be completed as soon as possible, we were concerned that this aggressive schedule would not permit sufficient analysis, documentation, and review to achieve adequate product content and quality and meaningful certification and accreditation processes. The dates by which NIST's units were to receive a risk assessment methodology had passed, yet the methodology had not been provided to the units. As all future dates depended on the risk assessments, this delay affects the entire schedule.

In its response to our draft report, NIST stated that the due date for completed system accreditations had been extended to September 30. It further stated that in FY03, NIST's IT security officer will conduct an independent review of certified and accredited systems and make recommendations to the NIST CIO. Given the complexity and importance of the activities required to accomplish certification and accreditation, including testing the security controls to ensure that they perform as intended, we remain concerned that even with the schedule extension, there is not enough time to adequately complete all of the requisite activities and documentation. We urged NIST to consider the accreditations provisional until there is confirmation that each system has all needed security controls and that these controls have been tested to ensure they perform as intended.

The FISCAM review (conducted as part of the audit of the Department's FY01 financial statements) found a similar lack of risk assessments, approved security plans, and certification and accreditation. It also noted that NIST needs to strengthen controls over physical access to the data center, improve password management, and better segregate duties. NIST's corrective action plan adequately addresses all of these areas.

NOAA. OAR and NMFS had performed risks assessments; NESDIS and NOS provided only hazard matrices, which are useful for evaluating the impact of hazards or threats to a system, but do not give enough detail for determining needed security controls or conducting certification activities. We did find one exception—a NESDIS system for which a risk assessment identified vulnerabilities and provided recommendations to mitigate them.

All of the NOAA offices we reviewed had up-to-date security plans whose content and format were generally consistent with NIST guidance and that were approved (signed and dated) by an IT security officer. However, some of the plans provided by NESDIS, NMFS, and NOS had been updated after the Department had issued a revised password policy, but did not comply with the policy.

Although all NOAA systems that we reviewed had current certifications and accreditations, only one (an OAR system) had evidence of security testing and evaluation[6]—an essential component of certification. Moreover, the seven NESDIS systems that we reviewed were only accredited in July, after we had requested documentation. In one instance, the security plan was approved after the system was certified, although certification should not occur without an approved security plan, and the system was accredited on the same day the security plan was approved. For five of these systems, security plan approval, certification, and accreditation occurred on the same day. The activities required for certification and accreditation would normally span a period of months; in the absence of any concrete evidence that indicates that security testing and evaluation had been performed, NESDIS' abbreviated timetable calls into question the validity of its certification and accreditation process.

Certification actions may be scaled to the level of information security being evaluated, but they must be sufficient to confirm that the security features of the software, firmware, and hardware have been implemented as intended and perform properly, and that the operational sites comply with requirements for physical, procedural, and communications security. This confirmation cannot be achieved without some amount of testing. Certification denotes that systems meet their documented information security requirements; to ensure that they continue to do so throughout their life cycle, they must be recertified at least every 3 years. Accreditation signifies that the responsible senior manager understands and accepts any residual risk associated with the system. Unless the certification and accreditation processes are rigorous, the assurances these credentials are intended to impart will be illusory.

[6] In response to our request for security test and evaluation materials, NOAA provided documentation for several additional systems. However, the material provided was generally limited to monitoring security aspects of day-to-day operations and did not specifically pertain to security testing and evaluation. Examples of what was provided include review of audit logs, analysis of intrusion detection system results, and analysis of network vulnerability scanner output.

The FISCAM review found that for its financial systems and networks, NOAA needs to establish a security management structure, improve account management, implement better physical and environmental controls, improve its firewall policy, establish software change control procedures for the firewall and other software, and implement segregation of duties. NOAA's corrective action plan adequately addresses these issues with the exception of the security management structure and segregation of duties.

NTIA. The operating unit had conducted risk assessments on the two systems for which we requested documentation, and provided security plans (which it considers approved) for both systems as well. The content and format of these plans are generally consistent with NIST guidance, but like ITA and BIS, NTIA lacks a formal plan approval process. Neither system had undergone security testing and evaluation or certification and accreditation.

FISCAM Findings for Additional Operating Units

Issues identified by the FISCAM reviews for additional operating units are summarized below. In general, the corrective action plans, if implemented appropriately, will address the information security weaknesses that were found. In some cases, actions have already been taken and the issues have been resolved.

Census. Of the eight systems reviewed, one did not have an approved risk assessment and all but one lacked an approved security plan (although the remaining seven systems had draft plans that generally followed NIST guidance for format and content). One system was accredited, and the rest were operating without accreditation, including four whose interim accreditations had expired. The review identified weaknesses in access controls and physical security and noted that Census had yet to prepare corrective action plans to address findings and recommendations reported by external organizations that performed security assessments for Census.

Economic Development Administration. No significant problems were found.

National Technical Information Service. Problems were cited with access controls and lack of a formal systems development life cycle process.

Office of the Secretary (Commerce Administrative Management System, or CAMS). CAMS lacked a completed risk assessment, approved security plan, and procedures for performing employee background checks and periodic reinvestigations. The system needs stronger password procedures for expeditiously terminating access by departing personnel, improved management of change request documentation, and stronger security measures for distributing source code.

V. Information Security Requirements Need to Be Included in IT Service Contracts

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

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

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

In addition, the Department's draft information security program policy provides guidance to protect sensitive systems and information in contracting for IT resources and services. We believe this policy will be effective with the addition of several suggestions we made on the draft. The Department CIO's office is planning to work with a contractor to develop a web-based training module on information security for contracting officers and contracting officer's technical representatives.

VI. Progress Is Being Made Toward Establishing an Effective Department-wide Information Security Program, Evaluating Performance, and Ensuring Employee Training

GISRA gives the Department CIO responsibility for developing and maintaining an agencywide information security program; ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques; and providing relevant training to personnel with significant information security responsibilities. To carry out its information security responsibilities, the Department CIO reallocated staff from lower priority areas to information security and critical infrastructure protection, increasing from 4 members in FY00 to 10 in FY02, and obtained funds in FY02 for contractor support. The Department's CIO office has implemented a compliance review program and corrective action oversight and tracking process, which should significantly improve information security. It is also preparing an information security program policy. Although information security awareness programs have been conducted Department-wide, additional efforts are needed to ensure that employees with significant information security responsibilities receive adequate specialized training and education. Finally, the operating units need to do a better job of identifying security risks and controls throughout the system life cycle so that security expenditures can be better estimated and justified.

A. A Draft Information Security Program Policy Has Been Developed and a Compliance Review Program Implemented

In last year's evaluation, we reported that the Department's information security policy needed to be updated and expanded. Commerce subsequently revised the policy and it is being circulated in draft for departmental review. The policy identifies the Department's requirements for information security programs and gives guidance for establishing such programs within the operating units—and is thus an essential tool for developing unit-specific policies and procedures to implement departmental and federal requirements.

Our review of NIST's information security program underscored the importance of having a Department-wide policy. We found that NIST's policy is missing critical control elements. Specifically, it does not assign responsibilities to the director of NIST and to the CIO for developing, implementing, and maintaining an agencywide security program. The policy also lacks key controls, including risk management, security control review, life cycle management, certification and accreditation, and contingency planning. As noted previously, when we completed our fieldwork at NIST in May, these controls had not been implemented. In its response to our draft report, NIST noted that the information security policy had been revised and was undergoing management review.

We reported last year that Commerce had performed few reviews to ascertain compliance with federal and departmental information security requirements. This year, the Department's CIO established a compliance review program that is intended to cover all operating unit information security programs and systems over a 3-year cycle. Personnel external to the operating unit and independent of the systems and programs being assessed conduct the compliance reviews. This year, reviews are being performed at Census, Bureau of Economic Analysis, and NOAA. For FY03, reviews are planned for BIS, EDA, Economics and Statistics Administration, ITA, Minority Business Development Administration, NTIA, and Office of the Secretary. These units were selected to validate that they had implemented actions to correct weaknesses and eliminate the vulnerabilities identified by GAO's FY01 information security review. Corrective actions resulting from GAO's review are scheduled for completion by September 30, 2002.

B. A Process for Maintaining and Tracking Corrective Actions Has Been Developed

Consistent with OMB's GISRA guidance, the Department's draft policy contains requirements aimed at ensuring that each operating unit maintains a plan for correcting identified information security weaknesses and tracks progress against the plan. Under the terms of the policy, the operating units must document the findings of external reviews (such as those conducted by OIG or GAO), self-assessments, and compliance reviews in a corrective action plan that details the unit's proposed steps for eliminating the deficiency, along with target completion dates, intermediate milestones, and actions that have been taken thus far. Staffs responsible for the system reviewed—typically the system owner and IT security officer—are to prepare the plan and submit it to the Department's IT security program manager for review. The plan will then be submitted to the operating unit CIO for approval. Changes to the target completion dates cannot be made without management approval.

IT security officers at each operating unit will track the status of the plan, with status reported to the Department's CIO office monthly. That office will maintain a database that tracks weaknesses identified by external reviews, and plans to also track weaknesses identified by the unit self-assessments. Officials in the Department CIO's office told us that the compliance reviews will validate, on a sample basis, whether adequate corrective actions were taken for weaknesses reported as resolved.

C. Training for Personnel with Significant Information Security Responsibilities Is Needed

The Department's draft policy stipulates that new employees and contractors must receive information security awareness training within 30 days of hire and prior to using any IT resource, as well as whenever a significant change in the information security policy or procedures occurs. All existing employees and contractors who have access to systems containing sensitive information are required to have annual refresher training. In the past year, at the direction of the Department's CIO, the operating units provided security awareness training for all employees and contractor personnel either through programs of their own or via web-based training made available by the CIO.

Less progress has been made in training personnel with significant information security responsibilities. The draft policy makes the operating units' IT security officer responsible for providing training materials, which must be compliant with NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* However, neither the draft policy nor any other identifies specific training requirements, and training appears to be inconsistent and incomplete among the operating units we reviewed.

In a move to address the training issue, Commerce formed a working group under its IT Security Officers Coordinating Committee.[7] The goal of the working group is to improve IT security awareness, training, and education Department-wide. The working group, according to its draft

[7] Membership consists of the Department's IT Security Manager and Critical Infrastructure Program Manager, all operating unit IT security officers including those from NOAA line offices, as well as a representative from the Office of Security and OIG.

charter, will specify functions requiring general and specialized IT security training, define minimum awareness activities to be implemented and topics to be covered in all training, identify training opportunities, and recommend a training policy.

In a related move, the Department CIO recently sponsored and paid for two important on-site training classes: Principles of Certification and Accreditation, and Roles and Responsibilities of the Designated Approving Authority. These classes covered the methodologies that NIST is using for updating its guideline on certification and accreditation. While the sessions could not accommodate all personnel who needed them, they were an important step in addressing a critical training area.

D. Capital Asset Plans Need to Include Additional Information on Information Security Costs and Requirements

OMB Circular A-11, which sets out requirements for preparing and submitting budget estimates, stipulates that capital asset plans (Exhibit 300s) for IT systems must describe the system's security measures and indicate whether they comply with GISRA. We examined the FY03 capital asset plans for 13 major departmental systems,[8] all operated by the units reviewed for this report, in light of the circular's section on security and privacy: nine of the systems were from NOAA, two were from NTIA, one was from NIST, and one from BIS. (ITA did not have any major systems.) Our purpose was to determine whether each capital asset plan (1) specified the system's projected security costs, (2) detailed how funds would be spent, and (3) adequately described the system's security requirements.

We found that most plans specified projected security costs, but only a few plans explained how these funds would be spent. Although most plans described the information security activities that need to be conducted over the system life cycle, some did not detail specific risks and security controls. We concluded that the operating units need to do a better job of identifying security risks and controls throughout a system's life cycle so that security expenditures can be better developed and justified.

VII. Conclusion

With leadership and commitment from Commerce senior management, the Department has made considerable progress over the past year toward establishing the foundation for an effective information security program. However, because information security did not receive enough attention in the past, the effort required to develop and direct a program that safeguards the approximately 600 diverse and complex Commerce systems is daunting. We believe the groundwork is being laid. The Department now needs to ensure that sound policies, procedures, and practices are implemented in the operating units, that each system has the needed information security measures, and that these measures are reviewed and maintained throughout the system's life cycle.

[8] The Department has a total of 37 major systems in FY03.