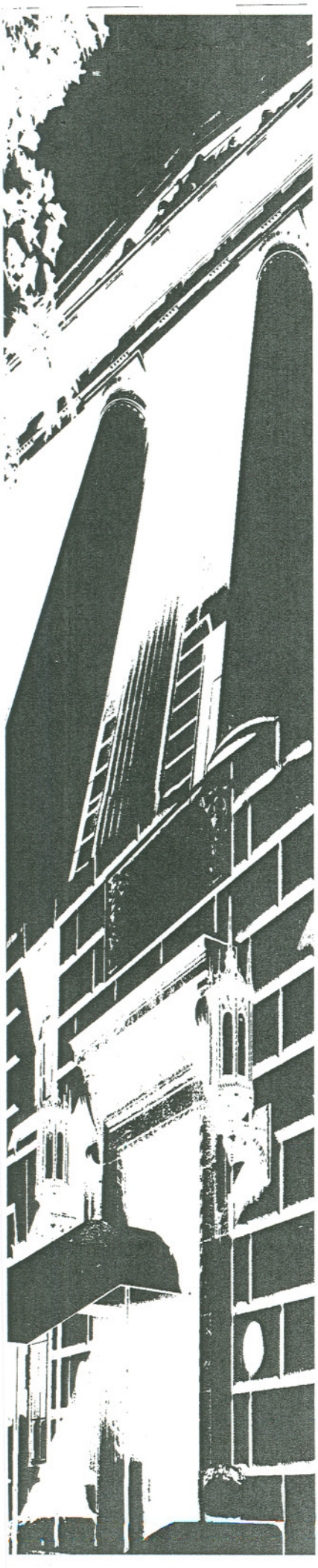


U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

PUBLIC RELEASE

UNITED STATES PATENT AND TRADEMARK OFFICE

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

Inspection Report No. OSE-14384-01-0002/September 2001

Office of Systems Evaluation

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report presents the Office of Inspector General's independent evaluation of the information security program of the Department of Commerce as required by the Government Information Security Reform Act.[1] The report's structure and content are designed to be responsive to the guidance provided by the Office of Management and Budget (OMB). The objective of our evaluation was to determine whether the Department's information security program and practices comply with the requirements of the act, which seeks to ensure proper management and security for the information resources supporting federal operations and assets.

Under the act, the Inspector General is required to perform an annual independent evaluation of the Department's information security program. The act also requires the Department to conduct an annual review of its information security program. In accordance with OMB guidance, both of these assessments are to be transmitted by the Secretary to OMB with the fiscal year 2003 budget materials. With the greater independence and flexibility provided by the American Inventors Protection Act of 1999 (P.L. 106-113), the United States Patent and Trademark Office (USPTO) is submitting its budget materials and information security review separate from the Department's. Therefore, an accompanying independent OIG information security evaluation is required. We are submitting the same independent evaluation for USPTO as for the Department because our evaluation addresses the status and issues associated with the Department as a whole, including USPTO. In addressing the Department as a whole, our assessment describes the Department's recent actions and plans to improve information security. Because USPTO is undertaking actions separate from the Department's to manage information security, we will review USPTO's information security program separately in next year's independent assessment.

Programs Reviewed and Methodology

Our evaluation is based on the collective results of OIG reviews and audits of (1) the Department's information security program functions assigned to the CIO, (2) the Department's implementation of the Critical Infrastructure Protection Program, (3) general controls associated with the information technology (IT) processing environment at various operating units conducted as part of OIG's fiscal year 2000 financial statements audits,[2] (4) security of the Census Bureau's Advance Retail Sales principal federal economic indicator, and (5) the use of persistent Internet cookies and web bugs on departmental Internet sites.

---

[1]Title X, subtitle G of the 2001 Defense Authorization Act (P.L. 106-398).

[2]Operating units reviewed were Bureau of the Census, Economic Development Administration, International Trade Administration, National Institute of Standards and Technology, National Oceanic and Atmospheric Administration, National Technical Information Service, and United States Patent and Trademark Office.

In order to determine how the agency integrates security into its capital planning and investment control process, we reviewed the capital asset plans and related budget request for fiscal year 2002 and the capital asset plans for fiscal year 2003. In order to determine the specific methods used by the Department to ensure that contractor-provided services are adequately secure, we reviewed a random sample of 40 contract actions for IT services from a universe of awards made by the Department during the period September 1998 through July 2001.

The general control reviews of financial systems and their related networks were conducted using GAO's *Federal Information System Controls Audit Manual* (FISCAM) as a guide and included penetration testing. The other evaluations were conducted using applicable federal laws and policies, as well as Department policies, as criteria.

Our evaluation also includes the results of reviews performed by other parties, which in accordance with OMB guidance, we determined were of sufficient quality, applicability, and independence. In particular, we used the results of the recent evaluation of information security in seven Commerce organizations,[3] conducted by the General Accounting Office (GAO), which included penetration testing of systems and networks based in the Herbert C. Hoover Building. We also used results of selected security assessments contracted for by individual operating units, namely, the Census Bureau, the Bureau of Economic Analysis, and the International Trade Administration.

In attempting to reconcile any differences between the OIG's independent evaluation and the USPTO's program review, it is important to note that USPTO's review, which was still ongoing as of early September, is based on self assessments, which were impossible for us to validate in the available time frame.

We did not include an audit of the evaluation of classified systems as required by the act because such an evaluation has not been conducted and therefore was not available from the Department. We plan to address these systems in next year's report. We are currently evaluating the information security program functions of the Deputy Assistant Secretary for Security that are associated with classified systems and will provide our findings in next year's report, as well.

New Department Emphasis on Information Security to Address Pervasive Weaknesses

Information security weaknesses throughout Commerce have prompted us to identify information security as one of the Department's top 10 management challenges. In addition to our own observations, GAO's recently completed penetration testing of the Commerce headquarters building revealed pervasive computer security weaknesses that place sensitive Commerce systems at serious risk.

---

[3]The Commerce organizations reviewed by GAO were the Office of the Secretary, the Bureau of Export Administration, the Economic Development Administration, the Economics and Statistics Administration, the International Trade Administration, the Minority Business Development Agency, and the National Telecommunications and Information Administration.

Recognizing the severity of this issue, the Department is making a concerted effort to improve information security. In July 2001, the Secretary directed secretarial officers and operating unit heads to give information security high priority, sufficient resources, and their personal attention. The Secretary's IT management restructuring, which recently took effect, is designed to increase the authority and effectiveness of the Department and operating unit CIOs. An IT security task force was recently formed, under the direction of the Deputy Secretary, to develop a comprehensive information security program plan for the Department.

Another step toward strengthening information security occurred in June 2001, when the Office of the CIO, the Office of Security, and the 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.

Evaluation Findings

Our evaluation found that because information security did not receive adequate attention in the past, significant weaknesses exist in policy, implementation, and oversight. Consequently, substantial efforts will be required to develop and oversee an effective information security program. Our findings are summarized below:

- **The Department Needs to Establish a Process to Report Security Deficiencies as Material Weaknesses.** The Security Act requires reporting of significant deficiencies in security policy, procedures, or practices as a material weakness. Circular A-130, *Management of Federal Information Resources*, requires operating units to identify security deficiencies pursuant to Circular A-123, *Management Accountability and Control,* and the Federal Managers' Financial Integrity Act if it is determined that there is no assignment of security responsibility, no security plan, or no accreditation. We found deficiencies associated with these elements throughout the Department that should be evaluated to determine whether they are material weaknesses. The determination to report a material weakness should depend on the risk and magnitude of harm that could result from the weakness. However, the Department lacks a policy or process for reporting information security deficiencies as material weaknesses. The Office of the CIO, along with the operating units, need to immediately identify the most critical departmental systems, define a reporting strategy, and specify milestones.

  Management control weaknesses which, in our opinion, pose a risk or a threat to the internal control systems of an audited entity must be identified and reported, even if the management of the audited entity would not report the weaknesses outside the agency. Our fiscal year 2000 financial statements audits concluded that four operating units had management control weaknesses in system security that rose to the level of "reportable

conditions."[4] Taken together, these conditions, combined with the Department's lack of an integrated financial management system, constituted a material weakness in the audit of the consolidated financial statements. (See page 7.)

- **Additional Efforts Are Needed to Improve Risk Assessment, Security Planning, and Test and Evaluation.** The Security Act requires the head of each agency to ensure that appropriate senior agency officials are responsible for assessing the information security risks associated with the operations and assets for programs and systems over which they have control, determining the levels of information security appropriate to protect such operations and assets, and periodically testing and evaluating information security controls and techniques. We found shortcomings in all of these areas.

  Our FISCAM reviews found entitywide security program planning and management needed improvement at all seven locations audited. Likewise, in reviewing 94 sensitive systems in the Department, GAO found that only 3 had documented risk assessments, 1 of which was still in draft and that only 7 had security plans, none of which had been approved by management. GAO also found that none of the systems were accredited.[5] The security assessments contracted for by individual operating units found a lack of documented policies, risk assessments, and security plans, as well as a lack of system accreditations. Operating unit self-assessments conducted in the Summer/Fall 2000 time frame, with oversight by the CIO's office, revealed that for the total population of Commerce IT systems, only 28 percent had risk assessments, 54 percent had security plans, and 8 percent were accredited. Many evaluations also found that information security control techniques are not being periodically tested and evaluated.

  Our Critical Infrastructure Protection (CIP) Program review found that vulnerability assessments have been completed for only 22 of the 241 IT assets deemed to be part of the nation's critical infrastructure, and that plans for determining the controls needed to reduce the vulnerabilities and justify CIP budgets had not been prepared. The CIO's office has noted that these assessments, as well as other required CIP efforts, are part of the overall information security program and that the Department will revise its policy to reflect this approach.

[4]"Reportable conditions"represent significant deficiencies in the design or operation of an internal control.

[5]Accreditation is the authorization of a system to process information granted by a management official. By authorizing a system to process information, a manager accepts a certain level of risk associated with it.

Finally, our review of the security of the Advance Retail Sales principal economic indicator found issues concerning the designation of positions according to risk and sensitivity.[6] Some employees with advance knowledge of sensitive economic data that could affect or predict financial market activity do not always have the requisite risk classifications or background investigations, and some positions are designated according to national security sensitivity levels rather than the appropriate risk levels, which can lead to inappropriate background investigations. These issues exist elsewhere in Commerce and are the result of a lack of current departmental guidance. Therefore, Commerce's program for position designation needs to be updated and strengthened. (See page 7.)

- **Additional Efforts Are Needed to Achieve an Adequate Department-wide Security Program, Evaluate Performance, and Ensure Employee Training.** The Security Act gives the 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 training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities. We found that substantial improvements are needed in these areas.

  Developed before a major revision of the security requirements of OMB Circular A-130, the Department's information security policy is out of date and needs to be revised and expanded. While the Department's oversight of information security has improved recently, it has performed few information security reviews. As a result, many Commerce systems lack adequate procedures and control techniques, placing information and equipment at risk. Problems include serious, pervasive weaknesses in access controls, inadequate segregation of duties and change control, weak intrusion detection and auditing capabilities, systems running software that is out-of-date or lacks the necessary vendor patches, and inadequate physical security. Moreover, security training is not conducted on a rigorous or ongoing basis, and none of the operating units was able to give us the information we requested on the number of agency employees who received security training or the cost of providing such training. Finally, the Department needs to ensure that the privacy of visitors to its Internet sites is safeguarded by enforcing its policies concerning the use of persistent cookies and web bugs.[7] Toward this end, the Secretary has appointed a senior privacy advisor, who is tasked with ensuring that privacy laws and policies are being followed throughout the Department. (See page 10.)

---

[6]Risk classifications address the damage an individual could cause to the efficiency and integrity of government programs and operations, whereas sensitivity classifications address the potential impact on national security.

[7]Persistent Internet "cookies" are data stored on web users' hard drives that can identify users' computers and track their browsing habits. Web bugs are software code that can monitor who is reading a web page.

- **Procedures for Detecting, Reporting, and Responding to Security Incidents Should Be Improved.** The Security Act requires agencies to have documented procedures for detecting, reporting, and responding to security incidents. We found that only 4 of 15 operating units have a formal incident response capability, one of which became operational this August, and most operating units have not installed intrusion detection systems. In addition, most operating units have weak or nonexistent auditing capabilities. The lack of auditing, coupled with weak intrusion detection capabilities, make it difficult for operating units to know when a security incident has occurred or who was responsible. In addition, the Department's policy that specifies how information security incidents should be reported needs to be revised to include reporting to the OIG and to define what constitutes a reportable incident.

  Two recent actions should help to address these issues. First, the memorandum of agreement between the CIO's office, OSY, and the OIG specifies that the OIG is to be notified immediately regarding IT system incidents/intrusions, and it defines a process for incident response. Second, the Department has recently begun planning to form a computer incident response team that will cover the operating units that do not have a formal response capability. (See page 14.)

- **Capital Asset Plans Should Identify Security Requirements More Explicitly and Link Them to Security Cost Estimates.** For the fiscal year 2002 budget request, OMB began requiring agencies to identify and budget for the security measures and resources that will be needed to protect IT investments, both in the earliest planning stages and throughout the life cycle. Security costs are to be presented in Exhibit 53, "Agency IT Investment Portfolio," and capital asset plans must be provided (Exhibit 300) indicating whether the project's security has met the requirements of the Security Act and describing the security and privacy measures that will be used. We found that while better information on security was presented for fiscal year 2003, the analysis of security requirements, measures, and costs needs improvement. Security was addressed in most fiscal year 2002 capital asset plans, but several plans did not cover this topic, and most did not identify security costs. Security costs were also omitted from the OMB budget request for several projects having capital asset plans. The fiscal year 2003 capital asset plans tend to have more detailed discussions of security, although most still do not identify security costs. Moreover, many of the plans do not clearly identify what the security requirements are or how they will be addressed, and where costs are estimated, they do not describe the basis of the estimate. (See page 15.)

- **Refinements Needed to Critical Asset Identification.** The Security Act requires agencies to identify, prioritize, and protect critical assets within their enterprise architecture, including links with key external systems. We found that the reliability of the Department's asset inventory for the CIP program is questionable because of weaknesses in the methodology used to gather asset data, and three of the Department's largest operating units expressed concern that the inventory did not reflect the priority of their assets. To

identify the critical asset inventory, the Department planned for operating unit managers to be interviewed by a contractor supporting its CIP program, using a survey questionnaire. However, because of logistical and resource problems in arranging the large number of meetings necessary to complete the questionnaires, operating unit managers with direct responsibility for, and the most knowledge of, the assets generally were not interviewed. In addition, operating units are not considering risks associated with their network interconnections with external systems.

The federal Critical Infrastructure Assurance Office has developed criteria for identifying critical assets that consider how quickly the asset would have to be reconstituted in an emergency. By applying the new criteria, the CIO's office expects the number of assets on the list to be significantly reduced from its current level of 241, allowing it to focus attention on those that are most critical. (See page 16.)

- **The Department Needs to Provide Guidance and Develop Procedures To Ensure That Contractor-Provided IT Services are Secure.** The Security Act requires the head of each agency to be responsible for developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of agency information. Outsourcing of IT services, such as network support and website operations, is widespread, and the Department must ensure that contract documents for IT services contain provisions for ensuring that contractors comply with security regulations, guidance, and policy. We found that the Department's information security and acquisition policies contain little guidance for integrating security into acquisitions and that the Federal Acquisition Regulation does not focus on system and data security. As a result, many Commerce contracts contain no provision for security safeguards. (See page 17.)

- **Information Security Plan Is Frequently Not Carried Out Throughout the Life Cycle of Agency Systems.** The Security Act requires the head of each agency to ensure that the agency's information security plan is carried out throughout the life cycle of each agency system in order to safeguard the privacy, confidentiality, and security of federal information. The agency head is also to promote security as an integral component of each agency's business operations. As the foregoing discussion has shown, the Department's information security policies need to be updated, oversight needs to be strengthened, and agency managers and program officials need to ensure that effective security policies and procedures are implemented throughout the life cycle of every IT system.

  Information security has yet to become an integral component of the Department's business operations. As a result, fundamental responsibilities are frequently not carried out, including:

  (1) Identifying, assessing, and understanding the risk of the Department's IT assets,

(2) Determining security needs commensurate with the level of risk,
(3) Planning, implementing, and testing controls that adequately address the risk,
(4) Promoting continuing awareness of information security risk and providing appropriate training, and
(5) Continually monitoring and evaluating policy and control effectiveness of information security practices.

As described previously, the Department is making a concerted effort to improve information security and to make it an integral component of the Department's business operations. The Department's recent actions to improve information security—if accompanied by continued executive-level attention and adequate resources—are important steps in building the foundation for a more effective information security program. (See page 18.)

INTRODUCTION

On October 30, 2000, the President signed into law the Government Information Security Reform Act, Title X, subtitle G of the 2001 Defense Authorization Act (P.L. 106-398). Referred to by the Office of Management and Budget (OMB) as the Security Act, the law amends the Paperwork Reduction Act of 1995 by enacting a new subchapter on information security,[1] which primarily addresses its program management and evaluation aspects. The Security Act became effective on November 29, 2000, and expires in two years.

The Security Act requires: (1) annual agency program reviews; (2) annual independent OIG evaluations; (3) agency reporting to the Office of Management and Budget (OMB) the results of OIG evaluations, and (4) an annual OMB report to the Congress summarizing the materials received from agencies. For national security programs, the evaluation is to be performed by an entity designated by the Secretary of Defense, the Director of Central Intelligence, or another agency head as designated by the President, and the OIG is to conduct audits of the independent evaluations. Agencies are to submit this information beginning in 2001 as part of the budget process.

In accordance with OMB guidance, the OIG independent evaluation and agency program review are to be transmitted by the Secretary to OMB with the fiscal year 2003 budget materials. With the greater independence and flexibility provided by the American Inventors Protection Act of 1999 (P.L. 106-113), the United States Patent and Trademark Office (USPTO) is submitting its budget materials and information security review separate from the Department's. Therefore, an accompanying independent OIG information security evaluation is required. We are submitting the same independent evaluation for USPTO as for the Department because our evaluation addresses the status and issues associated with the Department as a whole, including USPTO. In addressing the Department as a whole, our assessment describes the Department's recent actions and plans to improve information security. Because USPTO is undertaking actions separate from the Department's to manage information security, we will review USPTO's information security program separately in next year's independent assessment.

BACKGROUND

Responsibilities of Commerce Organizations for Information Security

Two Department Organization Orders (DOOs) establish the major responsibilities for information security within the Department of Commerce. DOO 15-23 prescribes the functions and

[1]The terms *information security* and *information technology (IT) security* are used interchangeably in the federal government. To be consistent with the terminology of the Security Act and OMB, this report uses the term *information security*.

organization of the Office of the Chief Information Officer (CIO). It tasks the CIO with developing and implementing a Departmental information security program to ensure the confidentiality, integrity, and availability of information and information technology (IT) resources. The CIO's responsibilities include developing policies, procedures, and directives for information security and providing oversight of the Department's operating units. The information security program is the responsibility of the IT Security Program Manager under the direction of the CIO's Office of Information Policy, Planning and Review.

DOO 20-6, which defines the functions and responsibilities of the Deputy Assistant Secretary for Security, assigns to this official responsibility for the operation, implementation, and review of information security throughout the life-cycle development of IT systems. The Deputy Assistant Secretary is also responsible for policies and procedures for safeguarding classified and sensitive documents and information, for the security accreditation of IT systems,[2] and for communications security.

In June 2001, the Office of the CIO, the Office of Security (OSY), and the 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.

The OIG's information security-related responsibilities originate with the Inspector General Act of 1978, which creates the OIGs as an independent and objective unit to conduct and supervise audits and investigations relating to programs and operations and to recommend policies for activities designed to promote economy, efficiency, and effectiveness in the administration of programs and operations. OIGs are also charged with preventing and detecting fraud and abuse in programs and operations. These authorities and functions are prescribed by DOO 10-13 for the Department of Commerce. In addition, DAO 207-10, which establishes policies and procedures for the initiation and processing of investigations, authorizes the OIG to investigate activity which may constitute a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health or safety. Under these authorities, the memorandum of agreement identifies the OIG's responsibilities for performing reviews of the Department's information security program and individual systems, including the annual independent evaluation of the program under the Security Act, and for conducting investigations of incidents and intrusions.

[2]Accreditation is the authorization of a system to process information granted by a management official. By authorizing a system to process information, a manager accepts a certain level of risk associated with it.

IT Management Restructuring

Each Commerce operating unit is to establish and implement an information security program using the Department's policy and guidance as the foundation. The Department's management of IT, including security, has been highly decentralized, as is its IT infrastructure. As GAO has recently pointed out, although the Commerce IT Review Board[3] approves major acquisitions, most operating units have their own IT budgets and act independently to acquire, develop, operate, and maintain their own infrastructure. Commerce has 14 data centers, diverse hardware platforms and software environments, and 20 independently managed e-mail systems. The operating units also develop and control their own individual networks to serve their specific needs.
In 1999, Commerce's former CIO initiated an effort to restructure IT management to increase the Department's control over information technology within the operating units. However, the restructuring was not implemented until June 2001, after the CIO had resigned and an acting CIO appointed. On June 13, 2001, the Secretary of Commerce directed secretarial officers and heads of operating units to implement the Department of Commerce IT Restructuring Plan designed to strengthen the Department's IT management. The plan:

- Requires the Department CIO to report to the Secretary.

- Requires each operating unit to establish a CIO, who will report to the head of the operating unit (Under Secretary, Assistant Secretary, Director, or Administrator) or principal Deputy, and to the Department's CIO.

- Gives operating unit CIOs responsibility for advising the operating unit on all aspects of IT and for developing and recommending policies for managing IT within the unit, consistent with departmental policies and guidelines.

- Gives operating unit CIOs line authority and responsibility for centralized IT functions.

- Gives operating unit heads (or their designee), in consultation with the Department's CIO, responsibility for establishing the performance plan and evaluating the performance of each operating unit CIO.

- Gives operating unit CIOs responsibility to establish and evaluate a critical element of the performance plan for the most senior IT manager for those IT personnel who do not report to the CIO.

[3]Members of the board include the Department CFO, Department CIO, Deputy CIO, Head of Budget, Director for Acquisition Management, Director of Human Resources Management, Digital Department Director, Major Operating Unit CIOs (NIST, NOAA), and smaller operating unit CIOs (ITA, NTIA).

- Requires that operating unit CIOs concur in the unit's budgeting and expenditure of funds for IT.

New Department Emphasis on Information Security to Address Pervasive Weaknesses

Information security weaknesses throughout Commerce have prompted the OIG to identify information security as one of the Department's top 10 management challenges. In addition to our own observations, the GAO recently completed penetration testing of the Commerce headquarters building and reported that pervasive computer security weaknesses place sensitive Commerce systems at serious risk.

Recognizing the severity of this issue, the Secretary has placed a new focus on information security. To emphasize its importance in the restructuring, on July 27, 2001, the Secretary issued a memorandum to secretarial officers and heads of operating units stating that information security should be given high priority and sufficient resources and that these officials are expected to personally invest the time necessary to assure full compliance with the information security improvement directives coming from the IT management restructuring plan. In addition, on July 23, an IT Security Task Force was established, under the direction of the Deputy Secretary, to develop a comprehensive information security program plan, including recommendations on functions to be carried out at both the departmental and operating unit levels.[4] The task force has also been asked to identify the highest priority information security tasks not currently being performed for immediate implementation. The task force is scheduled to conclude its work by September 30, 2001.

OBJECTIVES, SCOPE, AND METHODOLOGY

This report presents the results of our independent evaluation of the Department's information security program. The objective of our evaluation was to determine whether the Department's security program and practices comply with the requirements of the Government Information Security Reform Act, which seeks to ensure proper management and security for the information resources supporting federal operations and assets. Our evaluation is based on the collective results of OIG reviews and audits of (1) the Department's information security program functions assigned to the CIO, (2) the implementation of the Critical Infrastructure Protection (CIP) Program, (3) general controls associated with the IT processing environment at various operating units conducted as part of OIG's fiscal year 2000 financial statements audits, (4) security of the Census Bureau's Advance Retail Sales principal federal economic indicator, and (5) the use of persistent Internet cookies and web bugs on departmental Internet sites.

[4]Members of the IT security task force include the Commerce Acting CIO, Commerce Office of the CIO staff members, a representative from the Office of General Counsel, a representative from OSY, Census CIO, Census IT Security Officer, BXA CIO, NOAA IT Security Officer, NOAA Office of the CIO staff members, BEA IT Security Officer, ITA CIO, NTIA CIO, and representatives of the National Security Agency.

The general control reviews of financial systems and their related networks were performed for the following organizations:

- Bureau of the Census.
- Economic Development Administration (EDA).
- International Trade Administration (ITA).
- National Institute of Standards and Technology (NIST).
- National Oceanic and Atmospheric Administration (NOAA).
- National Technical Information Service (NTIS).
- United States Patent and Trademark Office (USPTO).

In order to determine how the agency integrates security into its capital planning and investment control process, we reviewed the capital asset plans and related budget request for fiscal year 2002 and the capital asset plans for fiscal year 2003. In order to determine the specific methods used by the Department to ensure that contractor-provided services are adequately secure and meet the requirements of the Security Act, OMB policy, and other related security guidance and policy, we selected a random sample of 40 contract actions for IT services from a universe of awards made by the Department during the period September 1998 through July 2001. We reviewed applicable contract files, including planning documents, work statements, and contract terms, conditions, and clauses.

The general control reviews of financial systems and their related networks were conducted using GAO's *Federal Information System Controls Audit Manual* (FISCAM) as a guide and included penetration testing. They are referred to in this report as FISCAM reviews. The other evaluations were conducted using applicable federal laws and policies, as well as Departmental policies as criteria.

Our evaluation also includes the results of reviews performed by other parties, which in accordance with OMB guidance, we determined were of sufficient quality, applicability, and independence. In particular, we used the results of GAO's recent evaluation of information security in seven Commerce organizations, which included penetration testing of systems and networks based in the Herbert C. Hoover Building.[5] We also used results of selected security assessments contracted for

[5]The Commerce organizations reviewed by GAO were the Office of the Secretary, the Bureau of Export Administration, the Economic Development Administration, the Economics and Statistics Administration, the International Trade Administration, the Minority Business Development Agency, and the National Telecommunications and Information Administration.

by individual operating units, namely, the Census Bureau, the Bureau of Economic Analysis, and ITA. A bibliography of sources used for this evaluation is presented in the appendix. Where appropriate, we have updated the findings in our reports through discussions with the Acting CIO and Office of the CIO officials responsible for the information security program.

In attempting to reconcile any differences between the OIG's independent evaluation and the USPTO's program review, it is important to note that USPTO's review, which was still ongoing as of early September, is based on self assessments, which were impossible for us to validate in the available time frame.

We did not include an audit of the evaluation of classified systems in this report because although such an evaluation is required by the Security Act, it has not yet been conducted for the Department's classified systems and therefore was not available for review. We plan to address these systems in next year's report. We are currently evaluating the information security program functions of the Deputy Assistant Secretary for Security that are associated with classified systems and will provide our findings in next year's report, as well.

The structure and content of this report are designed to be responsive to the guidance provided by OMB, *Reporting on the Government Information Security Reform Act.* This report is being issued in final because it is based primarily on prior work of the OIG that has been presented in previous audit and inspection reports and because it makes no recommendations.

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

FINDINGS

I. The Department Needs to Establish a Process to Report Security Deficiencies as Material Weaknesses

The Security Act requires reporting of significant deficiencies in security policy, procedures, or practices as a material weakness. Our review of the Department's information security policy and oversight found that the policy has no provision for reporting such deficiencies as material weaknesses. Failure to provide such reporting could result in a lack of management attention to unacceptably high security risks. Circular A-130, *Management of Federal Information Resources,* requires operating units to identify security deficiencies pursuant to Circular A-123, *Management Accountability and Control,* and the Federal Managers' Financial Integrity Act if it is determined that there is no assignment of security responsibility, no security plan, or no accreditation. We found deficiencies associated with these elements throughout the Department that should be evaluated to determine whether they are material weaknesses. The determination to report a material weakness should depend on the risk and magnitude of harm that could result from the weakness.

We recommended that security deficiencies be reported as material weaknesses when warranted. The CIO's office agreed, but expressed concerns about its ability to implement the recommendation and proposed establishing a senior management council as a forum for assessing and monitoring deficiencies as suggested in OMB Circular A-123. We believe that this is an appropriate approach, but no progress has been made since we completed our review in March. The Office of the CIO, along with the operating units, should immediately identify the most critical departmental systems, define a reporting strategy, and specify milestones.

Management control weaknesses which, in our opinion, pose a risk or a threat to the internal control systems of an audited entity must be identified and reported, even if the management of the audited entity would not report the weaknesses outside the agency. Our fiscal year 2000 financial statements audits concluded that four operating units had management control weaknesses in system security that rose to the level of "reportable conditions."[6] Taken together, these conditions, combined with the Department's lack of an integrated financial management system, constituted a material weakness in the audit of the consolidated financial statements.

II. Additional Efforts Are Needed to Improve Risk Assessment, Security Planning, and Test and Evaluation

The Security Act requires that the head of each agency ensure that appropriate senior agency officials are responsible for assessing the information security risks associated with the

[6]"Reportable conditions" represent significant deficiencies in the design or operation of an internal control.

operations and assets for programs and systems over which such officials have control, determining the levels of information security appropriate to protect such operations and assets, and periodically testing and evaluating information security controls and techniques. Our evaluation found serious shortcomings in all of these areas. As described previously, the Department recognizes the importance of addressing these problems and has recently initiated efforts to do so. However, because information security did not receive adequate attention in the past, substantial efforts will be required to develop and oversee an effective information security program.

A. Fundamental Security Program Elements Are Incomplete, Outdated, or Nonexistent

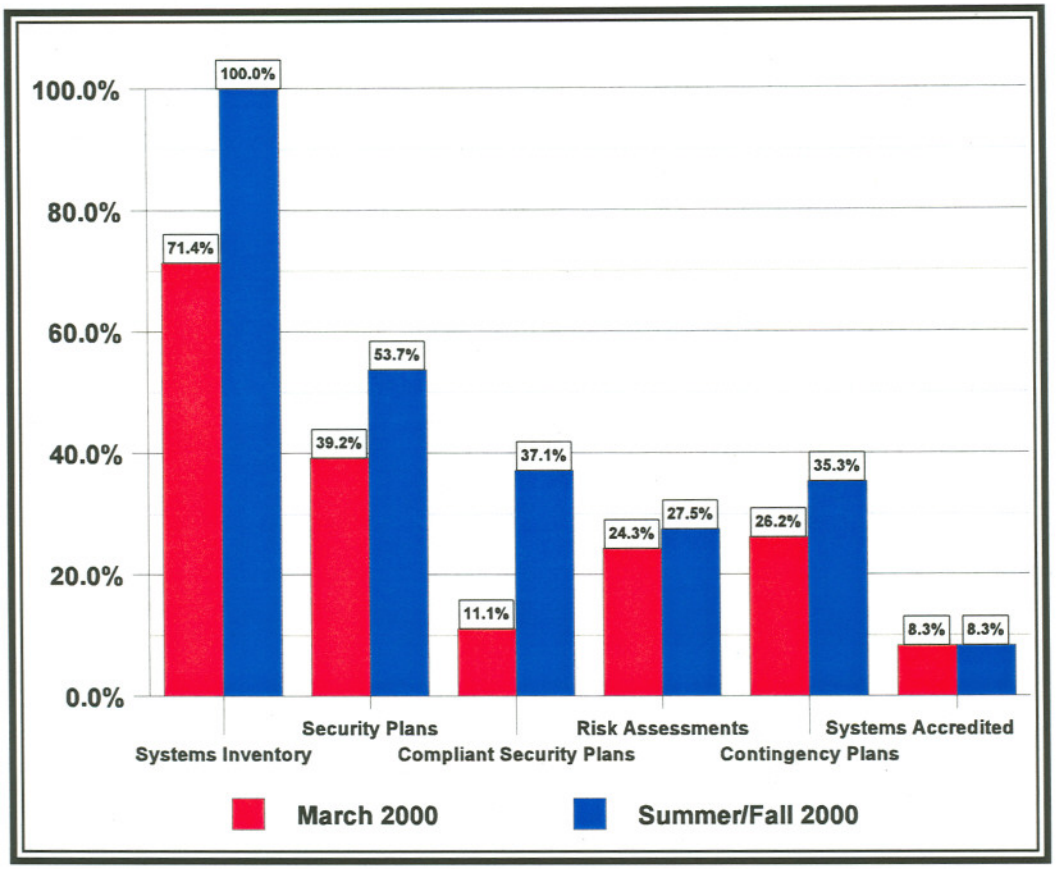
Our FISCAM reviews, the GAO evaluation, and the operating unit assessments found widespread problems in security planning and program management. These reviews found that in many operating units, risk assessments and security plans were outdated or nonexistent, and when they did exist, they frequently had not been finalized or approved by management. The reviews also found that the effectiveness of information security control techniques is not being periodically tested and evaluated for most Commerce IT systems. Our FISCAM reviews found that entitywide security program planning and management needed improvement at all seven locations audited. Likewise, in reviewing 94 sensitive systems in the Department, GAO found that only 3 had documented risk assessments, 1 of which was still in draft.

GAO also found that of the 94 systems reviewed, only 7 had security plans, none of which had been approved by management, and that none of the systems were accredited. The security assessments contracted for by individual operating units provided similar findings, including a lack of documented policies, risk assessments, and security plans, as well as a lack of system accreditations. One review stated that the operating unit lacked a credible systems accreditation program.

As for IT assets deemed to be part of the nation's critical infrastructure, our review of the implementation of Presidential Decision Directive 63, the Critical Infrastructure Protection (CIP) Program, found that vulnerability assessments had been conducted for only 22 of 241 of these assets and that plans for determining the controls needed to reduce the vulnerabilities and justify CIP budgets had not been prepared. The CIO's office has noted that these assessments, as well as other efforts required by the directive, are part of the overall information security program and that the Department will revise its policy to reflect this approach. The CIO's office has recently told us that because additional staff have become available, it plans to give the CIP work priority attention by October 1, 2001.

Figure 1 summarizes the status of the Department's information security program as reported in our review of its IT policy and oversight. This data is based on self-assessments conducted by 15

Figure 1: Department of Commerce Information Technology Security Program Status



operating units, with oversight by the CIO's office, using the Federal CIO Council's Draft IT Security Assessment Framework. The status presented as of March 2000 shows the results of the initial assessments. The updated status is for the Summer/Fall 2000 time frame and reflects improvements resulting from an increased focus on information security by the Office of the CIO. Although the more recent data shows that improvements are being made and attention to security is increasing, it also shows the magnitude of work remaining. For the total population of Commerce IT systems, only 28 percent had risk assessments, 54 percent had security plans, and 8 percent were accredited, meaning that management, operational, and technical controls had been tested and evaluated and that management had understood and accepted the risk associated with operating the system.

B. Program for Designating Positions According to Their Risk and Sensitivity Needs to Be Updated and Strengthened

The Department must ensure that employees having access to sensitive information and systems have appropriate, up-to-date background investigations and that positions are accurately designated according to their potential impact on government programs, operations, or national security. The requirements for performing these responsibilities are prescribed in 5 Code of Federal Regulations Part 731, *Suitability*; 5 CFR 732, *National Security Positions;* OMB Circular A-130; and the Computer Security Act. Our evaluation of the security of the Advance Retail Sales principal federal economic indicator found problems with position risk and sensitivity designations for personnel having access to sensitive information and systems. Specifically, some employees with advance knowledge of sensitive economic data that could affect or predict financial market activity do not always have the requisite risk classifications or background investigations.[7] Also, some positions of public trust are designated according to national security sensitivity levels rather than the appropriate risk levels, which can lead to inappropriate background investigations.

These issues exist elsewhere in Commerce and are the result of a lack of current departmental guidance on designating positions according to their level of risk and sensitivity. As a result, risk levels for some positions are inconsistent with their levels of responsibility and trust, some employees have not had appropriate background investigations, and the Department cannot always identify what type of background investigation, if any, was performed. The guidance for classifying these positions needs to be updated, as do the records on employee background investigations.

III. Additional Efforts Are Needed to Achieve an Adequate Department-wide Security Program, Evaluate Performance, and Ensure Employee Training

The Security Act gives the agency 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 training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities. We found that significant improvements are needed in these areas.

Our review of the Department's information security policy and oversight found that over the past several years the Office of the CIO has increased its focus on information security and devoted additional resources to it. In 1999 the CIO's office assessed information security planning Department-wide and as discussed previously, oversaw operating unit self-assessments

[7]Risk classifications address the damage an individual could cause to the efficiency and integrity of government programs and operations, whereas sensitivity classifications address the potential impact on national security.

in 2000. As a result of these reviews, operating unit compliance with security requirements has increased. However, because information security did not receive enough attention in the past and security demands continue to escalate, a sizable backlog of work and issues has accumulated.

A. The Department's Information Security Policy Needs to Be Revised and Expanded

Our review of the Department's information security policy and oversight, as well as the GAO review, found that the Department's information security policy is out of date and needs to be revised and expanded. It was developed in 1993 and 1995, before a significant revision of OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, "Security of Federal Automated Information Resources." It is missing important components because it has not kept pace with recent trends in technology usage and related security threats. The Department's policy must be current and complete because it is used by the operating units as the foundation for their general policy and to write system-specific policy.

The major areas that need to be revised involve information security planning, certification of system controls, periodic reviews of individual systems, security incident reporting, risk assessment, contingency and disaster recovery planning, security awareness and training, authorization of systems to process sensitive information, and referencing of related federal IT requirements. In addition, issue-specific policy regarding Internet usage, e-mail, web security, and communications needs to be added. The outdated and incomplete policy may place additional workload on operating units and increase security risk to the Department's information. The CIO's office agreed to revise the outdated program policy and incomplete issue-specific policy for the Department's information security program, and the Department plans to have the recently convened IT security task force provide assistance.

B. Department Oversight Has Increased, but Additional Efforts Are Needed

Additional information security compliance procedures are also needed. Although compliance with information security requirements is beginning to improve, for several years departmental oversight was minimal. As a result, information security for many of the Department's systems has not been adequately planned, and information security reviews have not been performed. In addition, several operating units do not have adequate awareness and training programs or adequate capabilities for responding to information security incidents. In response to our recommendations, the Office of the CIO agreed to begin security reviews as soon as possible, continue the review program beyond the FY 2002 duration of the Security Act, and make specific security improvements at the operating unit level.

GAO pointed out that Commerce does not have an effective Department-wide information security management program to ensure that sensitive data and critical operations are addressed and cited as a key issue the lack of a strong centralized management function to oversee and coordinate Department-wide security-related activities. The Department intends for the IT restructuring to enable the security management program to be improved Department-wide.

C. Many Systems Lack Adequate Procedures and Control Techniques

One result of limited oversight and training is that many of the Department's systems do not have adequate procedures and control techniques applied to them. The consequences are perhaps most disturbing in the area of access controls, where the FISCAM, GAO, and operating unit penetration testing revealed serious, pervasive weaknesses. Effective access controls limit or detect access to computer resources (i.e., data, programs, equipment, and facilities), protecting them against unauthorized modification, loss, and disclosure—either deliberate or inadvertent—from both inside and outside sources. Problems were found in such areas as:

- Inadequate user identification and authentication,
- Weak password management,
- Excessive system administrative privileges given to employees,
- Systems configured with excessive file access privileges,
- Operating system configurations that unnecessarily exposed information to potential attackers,
- Improper system and firewall configurations that allowed network breaches and the potential for breaches,
- Uncontrolled and improperly configured ancillary devices, such as modems, that allowed firewalls to be circumvented, and
- Multiple Internet access points that confuse and complicate network management and make networks more vulnerable to intrusions.

Other problems include inadequate segregation of duties[8] and change control, weak intrusion detection and auditing capabilities that permit potential incidents to go undetected, and systems running software that is out-of-date or lacks the necessary vendor patches. The reviews also found inadequate physical security for servers and inadequate or informal policies and procedures for sanitizing and disposing of computer equipment, system backup, and disaster recovery.

---

[8]Segregation of duties prevents any one individual from controlling key aspects of computer-related operations and thereby conducting unauthorized actions or gaining unauthorized access to assets or records. It is achieved through policies, procedures, and organizational structure.

D. Department Must Safeguard Privacy of Visitors to Its Internet Sites

The Department also needs to ensure that the privacy of visitors to its Internet sites is safeguarded. In our evaluation to determine whether information was being collected relating to any individual's access or viewing habits on the Department's or its operating units' Internet sites, we found that although the majority of sites do not use persistent cookies,[9] there were several instances in which they were being used without a compelling reason and without the approval of the Secretary of Commerce, as required by Department and OMB policy. We also found a number of web pages using web bugs,[10] a mechanism that also raises security issues because web bugs can be used to download files from and upload files to a user's computer. Moreover, many of the operating units' privacy statements did not provide all of the information required by the Department's privacy policy.

As a result of our evaluation, the CIO's office issued a memorandum entitled *Use of "Web Bugs" on Commerce Web Sites,* which establishes a policy for web bugs similar to that which was already in effect for persistent cookies, and all of the cookies and web bugs we identified have been removed. The CIO's office also agreed to direct operating unit CIOs and senior management to implement a strategy to control the use of persistent cookies and web bugs and to certify annually that the operating unit is in compliance with the Department's applicable policies. In addition, the CIO's office agreed to direct operating unit CIOs and senior management to revise their privacy policy statements to make them compliant with the Department's privacy policy. Finally, the Secretary appointed a senior privacy advisor, who is tasked with ensuring that privacy laws and policies are being followed throughout the Department.

E. Security Training Is Not Conducted on a Rigorous or Ongoing Basis

Only 4 of the 15 operating units covered in the self-assessments reported having a formal information security awareness, training, and education program. GAO found inadequate security awareness and training, noting that the seven operating units it reviewed have informal programs, but none has documented training procedures that meet federal requirements for ensuring that security risks and responsibilities are understood by all managers, users, and system administrators. The reviews contracted for by the operating units reported similar findings. In fact, a security assessment conducted after the self-assessment for one of the units that reported having a formal training program concluded that there was no formal training and awareness program for users or administrators and that the security of the computer systems depended on the self-motivation of the system administrators. Throughout the Department, system administrators receive little if any security training, and training for IT security officers has been

[9]Persistent Internet "cookies" are data stored on web users' hard drives that can identify users' computers and track their browsing habits.

[10]Web bugs are software code that can monitor who is reading a web page.

largely informal. Finally, none of the operating units was able to give us the information we requested on the number of agency employees who received security training or the cost of providing such training.

IV. Procedures for Detecting, Reporting, and Responding to Security Incidents Should Be Improved

The Security Act requires agencies to have documented procedures for detecting, reporting, and responding to security incidents. However, only 4 of 15 operating units have a formal incident response capability, one of which become operational this August and is still in the process of developing its capabilities. Our FISCAM audits, our evaluation of the Advance Retail Sales indicator, the GAO review, and the operating unit assessments found a recurrent problem of weak or nonexistent auditing capabilities. Program and system managers either did not have auditing capability on their systems, had it disabled, or had it enabled but did not regularly review the results. Ineffective intrusion detection capabilities were identified by several reviews, including GAO's, which found that only two of seven operating units had installed intrusion detection systems. The lack of auditing, coupled with weak intrusion detection capabilities, make it difficult for operating units to know when a security incident has occurred or who was responsible. Moreover, GAO found that six of the seven operating units it reviewed had ad hoc processes and procedures for incident handling, despite the fact that in July 1999 guidance on how to prevent, detect, respond to, and report security incidents had been issued by the CIO's office.

The Department's policy that specifies how information security incidents should be reported needs to be revised to include reporting to the OIG. The current policy calls for operating units to notify the IT Security Manager within 24 hours and submit a written report as soon as possible after an incident has occurred. The OIG has been notified of some incidents through informal means, but reporting has been inconsistent. The policy should require OIG notification because of the responsibilities specified in the Inspector General Act, as amended, and Departmental Administrative Order 207-10 for IG investigations. The CIO's office has agreed to include reporting to the OIG in its revised policy, and the two offices are working together to determine what incidents should be reported.

In our review of the CIO's files of written incident reports from operating units, we observed that approximately 89 percent of the reports were filed by NOAA operating units. This suggests that to the extent that incidents are detected, many operating units may not be reporting them as required. In addition, the vast majority of reports were for unsuccessful access attempts that did not involve intrusion into the Department's systems, networks, or web sites and did not involve any manipulation, destruction, or loss of data or systems, or denial of service. We suggested that the Department consider changing its reporting requirements to include only those incidents that the operating units believe could be significant, such as actual intrusions, the detection of viruses, denial of service attacks, defacing of web sites, or repeated access attempts by the same address. Statistics on failed attempts could be kept by operating units and reported periodically.

Two recent actions should help to address these issues. First, the memorandum of agreement between the CIO's office, OSY, and the OIG specifies that the OIG is to be notified immediately regarding IT system incidents/intrusions, and it defines a process for incident response. Second, the Department has recently begun planning to form a computer incident response team that will cover the operating units that do not have a formal response capability. However, the definition of what constitutes a reportable incident must still be developed, and improved intrusion detection and auditing are needed to prevent incidents and make incident response more effective.

V. Capital Asset Plans Should Identify Security Requirements More Explicitly and Link Them to Security Cost Estimates

For the fiscal year 2002 budget request, OMB began requiring agencies to identify and budget for the security measures and resources that will be needed to protect IT investments, both in the earliest part of the planning of an investment and throughout its life cycle. Security costs are to be presented as a percentage of the total system or project investment in Exhibit 53, "Agency IT Investment Portfolio," and capital asset plans must be provided (Exhibit 300) indicating whether the project's security has met the requirements of the Security Act and describing the security and privacy measures that will be used.

For fiscal year 2002, the Office of the CIO requested that all IT budget proposals include life cycle costs for information security planning and maintenance and (1) identify the security measures that will ensure the confidentiality, integrity, and availability of the proposed IT investment, (2) describe how the security measures are commensurate with the risk or magnitude of harm that may result from the loss of the asset or its services, (3) describe how these security measures integrate with and support the operating unit's IT architecture, and (4) indicate what percentage of expenditures for this IT investment will be devoted to incorporating and maintaining the needed level of security. For fiscal year 2003, the CIO's office requested that as part of Exhibit 53, a summary and description of information security base funding and proposed new funding be submitted at a level that will help to ensure that adequate resources are dedicated to information security in each operating unit and that system and data integrity and continuity of operations are conducted at an acceptable level of risk.

To promote IT investments that are well planned and justified, each operating unit has an IT board that reviews all proposed investments. Capital asset plans are prepared for high visibility or high cost projects and are required to include a description of information security measures and resources. The plans must be approved by Commerce's Information Technology Review Board in order for the project to obtain funding.

While most fiscal year 2002 capital asset plans addressed security, several did not, and most did not identify security costs. Security costs were omitted from Exhibit 53 for several projects having capital asset plans. The fiscal year 2003 capital asset plans tend to have more detailed discussions of security, although most still do not identify security costs. Also, the plans that do

identify security costs provide the estimate as a percentage of the total investment, but do not show how these costs are distributed over time or what portion is applicable in the year of the budget request. Finally, many of the plans do not clearly identify what the security requirements are or how they will be addressed, and none describe the basis of the security cost estimate.

VI. Refinements Needed to Critical Asset Identification

The Security Act requires identifying, assessing, and understanding the risk of information systems on a continuing basis, and agencies must identify, prioritize, and protect critical assets within their enterprise architecture, including links with key external systems. Our report on critical infrastructure protection questioned the reliability of the minimum essential infrastructure, or critical asset, inventory—the list of IT-based and physical assets essential to the minimum operations of the economy—because of weaknesses in the methodology used to gather asset data.

Establishing the critical asset inventory is an important part of the requirements of the CIP program because it forms the basis for subsequent activities. Based on the inventory, the assets with the highest risk are given priority for further vulnerability assessment to determine the amount of risk exposure. A remediation plan can then be formulated to reduce the vulnerability. Remediation plans are also to be used to justify budget resources so that corrective actions can be implemented. If the inventory is not accurate, the Department's most vulnerable assets may not be recognized, and vulnerabilities may not be addressed in priority order. At the time of our evaluation of the CIP program, three of the Department's largest operating units had expressed concern that the inventory did not reflect the priority of their assets.

Although a systematic process was developed for formulating the inventory, data gathering was limited because few asset managers were interviewed or given adequate guidance on program criteria. A survey questionnaire was used to collect asset data, but operating unit managers with direct responsibility for, and the most knowledge of, the assets were generally not interviewed. The original plan was for operating unit managers to be interviewed by the contractor supporting the Department's CIP program and for the survey questionnaires to be completed by the contractor during the interviews. However, this did not occur because of logistical and resource problems in arranging the large number of meetings with operating unit managers necessary to complete the questionnaires. Instead, operating unit personnel usually completed the survey questionnaires themselves, with only a few interacting directly with the contractor.

As for links with key external systems, GAO's evaluation pointed out that operating units are not considering risks outside their immediate environment that affect the security of their systems, in particular, network interconnections with other systems. This can be a serious omission because vulnerabilities in one system can undermine the security of all of the systems to which it is connected.

The CIO's office agreed that the asset inventory needed refinement but said that this had been not done because of limited funding and staff resources. However, with additional resources becoming available, it plans to begin a reevaluation of the asset list by October 1, 2001. The federal Critical Infrastructure Assurance Office has added criteria for identifying critical assets that consider how quickly the asset would have to be reconstituted in an emergency. By applying the new criteria, the CIO's office expects the number of assets on the list to be significantly reduced from the current total of 241, allowing it to focus attention on those that are most critical.

VII. The Department Needs to Provide Guidance and Develop Procedures to Ensure That Contractor-Provided IT Services Are Secure

The Security Act requires the head of each agency to be responsible for developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency. Because outsourcing of IT services, such as network support and website operations, is widespread and increasing, the Department must ensure that contract documents for IT services contain provisions for ensuring that contractors comply with security regulations, guidance, and policy. However, we found that policy and procedures to be applied during the acquisition process to ensure information security are minimal. As a result, many contracts contain no provision for security safeguards.

Despite the fact that acquisition is a major phase in the life cycle of IT systems, the Department's information security and acquisition policies contain little guidance for integrating security into acquisitions. The Department's IT policy states that acquisition documents must contain specifications to assure adequate security requirements, but provides no explanation of the considerations and process for implementing this requirement. The Department has very little actual acquisition policy pertaining to security, and the guidance in the Federal Acquisition Regulation does not focus on system and data security, although it does address privacy issues.

A 1992 NIST publication, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials,* provides useful guidance for incorporating security requirements into the acquisition process. It stresses the need for program officials, users, computer security officers, and IT staff to work together, beginning with the planning phase, to ensure that security requirements are appropriate, incorporated in work statements and contract documents, and closely monitored during contract administration. Although this document needs to be updated to incorporate changes as a result of acquisition reform legislation, it remains an informative tool. However, contracting officers we spoke with were not even aware of its existence.

Our review of a random sample of 40 contract actions for IT services awarded by the Department during the period October 1998 through July 2001 found that as a result of the lack of appropriate guidance and policy, many of these contracts contained few, if any, provisions for the security of IT systems and relevant data. Our review of acquisition plans and requirements documents revealed that security was not a consideration during the planning and requirements specification phases and that most work statements also did not contain security requirements. Consequently, the Department cannot assure that contractor-provided IT services are secure and meet regulatory requirements.

VIII. Information Security Plan Is Frequently Not Carried Out Throughout the Life Cycle of Agency Systems

The Security Act requires the head of each agency to ensure that the agency's information security plan is carried out throughout the life cycle of each agency system in order to safeguard the privacy, confidentiality, and security of federal information. The agency head is to promote security as an integral component of each agency's business operations, along with IT architectures, as defined by the Clinger-Cohen Act of 1996.[11]

As the previous discussion has shown, the Department's information security policies need to be updated, oversight needs to be strengthened, and agency managers and program officials need to ensure that effective security policies and procedures are implemented throughout the life cycle of every IT system. Information security has yet to become an integral component of the Department's business operations. As a result, fundamental responsibilities are frequently not carried out, including:

- Identifying, assessing, and understanding the risk of the Department's IT assets,
- Determining security needs commensurate with the level of risk,
- Planning, implementing, and testing controls that adequately address the risk,
- Promoting continuing awareness of information security risk and providing appropriate training, and
- Continually monitoring and evaluating policy and control effectiveness of information security practices.

The Department has several mechanisms that can be used to foster security throughout the life cycle of each agency system. All operating units are required to develop and submit IT

[11]The Clinger-Cohen Act defines the term information technology architecture as an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals.

architectures or architecture plans, which are linked to their strategic and operational IT plans.[12] To be rated highly, investments proposed through the capital planning and investment process must conform to the operating unit's architecture, which should include information security requirements. In addition, agencies are required to identify and budget for the information security measures and resources that will be required to protect IT investments and to present this information in their capital asset plans. Increased attention to security in these plans, architectures, and budget requests would improve planning and implementation of security throughout the life cycle of Commerce systems.

Finally, as described previously, the Department is making a concerted effort to improve information security. The Secretary's recent memorandum to secretarial officers and agency heads emphasized the importance of information security and the need for their personal involvement. The Secretary's IT restructuring, including authorizing the CIOs of the operating units to concur in the budgeting and expenditure of IT funds, makes these officials a more integral part of the management team. The new IT security task force is concentrating on developing a comprehensive information security program plan. These actions represent important steps toward developing a Commerce information security program and making security a fundamental component of the Department's business operations.

[12]The purpose of the strategic IT plan is to describe in general terms how IT will be used to support the key program missions and goals defined in the organization's strategic plan. The purpose of the Operational IT plan is to provide a more detailed description of IT actions and investments planned and to support an investment analysis of these plans.

APPENDIX

Sources Used in This Report

OIG Reports

1. *Additional Security Measures Needed for Advance Retail Sales Economic Indicator,* OSE-12754, September 2001.

2. *Use of Internet "Cookies" and "Web Bugs" on Commerce Web Sites Raises Privacy and Security Concerns,* OSE-14257, April 2001.

3. *Additional Focus Needed on Information Technology Security Policy and Oversight,* OSE-13573, March 2001.

4. *Critical Infrastructure Protection: Early Strides Were Made, but Planning and Implementation Have Slowed,* OSE-12680, August 2000.

5. U. S. Department of Commerce, *Consolidated Financial Statements, Fiscal Year 2000,* FSD-12849-1-0001, March 2001.

6. Bureau of the Census, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-12850-0001, January 2001.

7. Economic Development Administration, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-12851-1-0001, January 2001.

8. International Trade Administration, *Review of General and Application System Controls Associated with the Fiscal Year 2000 Financial Statements*, FSD-12854-1-0001, January 2001.

9. National Institute of Standards and Technology, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-12859-1-0001, February 2001.

10. National Technical Information Service, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12857-1-0001, January 2001.

11. National Oceanic and Atmospheric Administration, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-12855-1-0001, December 2000.

12. United States Patent and Trademark Office, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-12858-1-0001, December 2000.

Other Materials

1. *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk,* Report to the Chairman, Committee on Energy and Commerce, House of Representatives, United States General Accounting Office, GAO-01-751, August 2001.

2. *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk,* by Robert F. Dacey, Director, Information Security Issues, United States General Accounting Office, Testimony before the Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce. GAO-01-1004T, August 3, 2001.

3. *U.S. Census Bureau Information Security Program Risk Assessment, Risk Assessment Report,* Computer and Hi-tech Management, Inc., October 2000.

4. *Information Systems Security Assessment of United States Department of Commerce, Bureau of Economic Analysis,* National Security Agency, November 2000.

5. *International Trade Administration Phase II Risk Vulnerability Assessment*, JAVIS Automation & Engineering, Inc., May 2001.