U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

PUBLIC RELEASE

OFFICE OF THE CHIEF INFORMATION OFFICER

Additional Focus Needed on Information Technology Security Policy and Oversight

Inspection Report No. OSE-13573/March 2001

Office of Systems Evaluation

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

INTRODUCTION 1

BACKGROUND 1

OBJECTIVES, SCOPE, AND METHODOLOGY 4

FINDINGS AND RECOMMENDATIONS 6

I. The Department's IT Security Policy Needs to Be Revised and Expanded 6
- A. Security plan criteria should be updated 7
- B. The requirements for certification should be revised 8
- C. Self-verification reviews should be encouraged 9
- D. IT security incidents should be reported to the OIG 9
- E. Risk assessment policy should be reconsidered 10
- F. Contingency and disaster recovery back-up planning should be reemphasized . 11
- G. Mandatory pre-access training should be highlighted 11
- H. Designated Approving Authority for nonclassified systems should be a management official 12
- I. Related federal requirements should be added 13
- J. Issue-specific policy concerning Internet usage, e-mail, web security, and communications should be added 14
- K. Recommendation 15
- L. CIO response and OIG comments 16

II. CIO Has Taken Steps to Improve IT Security, But Additional Efforts Are Needed 17
- A. Recommendation 22
- B. CIO response and OIG comments 23

APPENDIXES
- A. Glossary of IT Security Terms
- B. CIO Response to the Draft Report

EXECUTIVE SUMMARY

IT security is a growing concern in government as vulnerabilities, threats, and attacks grow with the dramatic increase in the number of government networks and use of the Internet. In 1997 the General Accounting Office identified IT security as "a new high-risk area that touches virtually every major aspect of government operations." Although there is no single action agencies can take to make their networks completely secure, there are steps that can be taken to mitigate risk, which include developing and overseeing an effective security program based on sound policy.

Commerce Department Organization Order 15-23, July 2000, tasks the Chief Information Officer (CIO) to develop and implement a Departmental Information Technology (IT) security program to ensure the confidentiality, integrity, and availability of information and IT resources. The CIO's responsibilities include developing policies, procedures, and directives for IT security and providing oversight of the Department's operating units.[1] The IT 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.

The objective of this inspection was to assess the effectiveness of the CIO's policy and oversight of the Department's IT security program, generally excluding classified systems, which are the primary responsibility of the Office of Security. We satisfied this objective by evaluating the CIO's compliance with laws and regulations governing IT security. We compared the Department's *Information Technology Management Handbook,* Chapter 10, "Information Technology Security," and attachment, "Information Technology Security Manual" with the criteria in the laws and regulations to evaluate the CIO's policy. We evaluated oversight by reviewing actions in the last three years related to CIO oversight of the Department's IT security program.

Over the past several years the CIO has increased its focus on IT security and devoted additional resources to this area. In 1999 the CIO assessed IT security planning Department-wide and in 2000 oversaw operating unit self-assessments. As a result of these reviews, operating unit compliance with security requirements has increased. However, because IT security did not receive enough attention in the past, policy and oversight need further improvements. Moreover, even though the CIO is taking steps to improve IT security, it is unclear whether the additional resources will be sufficient to adequately address this complex and growing challenge.

[1]Refers to bureaus, administrations, agencies, and sub-offices within the Office of the Secretary, including the Office of Inspector General.

The Department's IT Security Policy Needs to be Revised and Expanded

The CIO's policy is out of date because it was developed in 1993 and 1995, prior to a significant revision of Office of Management and Budget 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. It is important that the Department's policy is current and complete since it is used by the operating units as the foundation of their general policy and to write system-specific policy.

The major areas that need to be revised involve IT 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. These areas are discussed on pages 6 through 15. The outdated and incomplete policy may place additional workload on operating units and increase security risk to the Department's information. We recommend that the CIO revise the outdated program policy and incomplete issue-specific policy for the Department's IT security program as soon as possible (see page 15).

Additional IT Security Compliance Procedures Need to Be Implemented

Although the CIO has considerably improved IT security compliance recently, for several years Departmental oversight was minimal. As a result, IT security for many of the Department's systems has not been adequately planned, and IT security reviews have not been performed. In addition, several operating units do not have adequate awareness/training programs or adequate capabilities for responding to IT security incidents. A more complete discussion of IT security compliance is on pages 17 through 22.

The Government Information Security Reform Act requires the CIO to conduct annual reviews of IT security in 2001 and 2002 similar to the 2000 self-assessments it oversaw. In addition, we recommend that the CIO commit to a program of operating unit reviews as soon as possible that extends beyond the act's two-year review requirement. The reviews should determine whether all operating unit policy is in compliance with federal criteria, IT security awareness and training programs have been developed, and formal incident response capabilities have been implemented.

To ensure that IT security is planned and funded in future IT acquisitions, the CIO should work with the Department's Acquisition and Budget managers to ensure that IT-related procurement specifications include security requirements and that the requirements are included in operating

unit budgets. The CIO should also ensure that deficiencies in IT security are reported as material weaknesses as required by OMB Circular A-123, *Management Accountability and Control*, and the Federal Manager's Financial Integrity Act.

In spite of limited resources, the program should also include sampling of operating unit IT security documents to ensure that IT security planning for the Department's most critical systems is complete, systems are properly approved for processing information, the security controls in each system are reviewed periodically, and a mechanism exists for ensuring that only legal copies of software are being used (see page 22).

In the March 30, 2001, response to our draft report, the CIO agreed with all of our recommendations to improve IT security. Specifically, the CIO agreed to revise and expand the Department's IT security policy and plans to update the policy in the immediate future. The CIO also agreed to continue the IT security compliance review program beyond the FY 2002 duration of the Government Information Security Reform Act, to begin security reviews as soon as possible, and to make specific security improvements at the operating unit level. We recognize that during the past two years the CIO has significantly improved the Department's IT security program, but the program still lacks adequate staff to perform the critical IT security function.

The CIO agreed with our recommendation to report security deficiencies as material weaknesses when there is no assignment of security responsibility, no security plan, or no accreditation, but expressed concerns about the ability to implement this recommendation. We believe, however, that the CIO, along with the operating units, should identify the most critical departmental systems, define a reporting strategy, and specify interim milestones.

Even though the CIO is committed to performing IT security compliance reviews beyond the duration of Government Information Security Reform Act, the lack of adequate staffing will affect the breadth and depth of these reviews. In particular, the lack of adequate staffing will prevent the CIO from performing hands-on compliance reviews of operating units to fulfill OMB reporting requirements for FY 2001. Thus, as the CIO's response notes, reliance will be placed on the results of IT security self-assessments performed by the operating units using the Federal CIO Council's Security Assessment Framework.

The CIO's full response is included as Appendix B to this report.

INTRODUCTION

This report presents the results of our systems evaluation of the Department of Commerce information technology (IT) security program functions assigned to the Chief Information Officer (CIO). IT security issues regarding functions assigned to the Office of Security, primarily for the Department's classified information[2] systems, will be addressed in a subsequent, separate report.

Systems evaluations are reviews of system development, acquisitions, operations, and policy in order to improve efficiency and effectiveness. They focus on Department-wide computer systems and other technologies and address all project phases, including business process reengineering, and system definition, development, deployment, operations, and maintenance.

The evaluation was conducted in accordance with the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency, and was performed under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated May 22, 1980, as amended.

BACKGROUND

According to Department Organization Order 15-23, July 3, 2000, the CIO has Department-wide approval and risk management responsibility for automated information systems, including implementation of policies, plans, and rules, and in collaboration with the Deputy Assistant Secretary for Security, the security of information systems throughout their life cycle. The order tasks the CIO to develop and implement a departmental IT security program to ensure the confidentiality, integrity, and availability of information and IT resources, including developing policies, procedures, and directives for IT security. The order also assigns the CIO explicit oversight responsibility for operating units and the Office of the Secretary.[3]

[2]Information which requires protection against unauthorized disclosure and is marked to indicate its classified status pursuant to Executive Order 12958, *Classified National Security Information*, April 1995. Classified information is generally afforded more stringent security.

[3]For ease of reference, the words "operating unit(s)" in this report will include operating segments of the Department of Commerce including bureaus, administrations, agencies, and sub-offices within the Office of the Secretary, including the Office of Inspector General.

The CIO developed program-level policy[4] that established the Department's IT security program, including some issue-specific policy focusing on topical areas of importance, such as malicious software (viruses). The Department's program-level and issue-specific policy is used to formulate operating unit policy, including system-specific policy. The CIO's IT security program is the responsibility of the IT Security Manager and a staff of three under the direction of the Office of Information Policy, Planning and Review. The IT Security Manager is responsible for developing IT security policy and overseeing operating unit IT security programs.

IT security is a growing concern in government as vulnerabilities and attacks grow with the dramatic increase in the number of government networks and use of the Internet. To guard against outside attackers is not enough. While most people are aware of external threats from hackers[5] and computer viruses, a significant number of attacks on computer systems come from those who have legitimate access to the networks. It is impossible to gauge the true number of attempted or actual intrusions into federal networks because there is no central repository for such information, but there are indications that the problem is getting worse. Risks to government information have prompted federal agencies to spend billions of dollars on IT security.

Although there is no single action agencies can take to make their networks completely secure, there are steps that can be taken to mitigate risk. There are many architecture-based improvements, such as firewalls,[6] that agencies can add to their systems to improve security. There are also augmentations to an agency's IT security efforts, such as establishing an incident response capability[7] that provides a mechanism for identifying and resolving IT security problems. However, the foundation of effective security programs is the establishment and enforcement of sound IT security policy. Some of the most effective and least costly controls to protect sensitive information, such as properly identifying and authenticating users and limiting

[4]Policy used to create an organization's computer security program. Program-level policy is supported by issue-specific policy that addresses specific issues of concern, and system-specific policy that focuses on decisions taken by management to protect a particular system. System-specific policy is often implemented through the use of access controls.

[5]Over time, this term has been widely accepted as describing someone who breaks into computer systems.

[6]A device that protects a private network from the public part. Usually, a computer is set up to monitor traffic between an Internet site and the Internet. It is designed to increase security by keeping unauthorized outsiders from tampering with a computer system.

[7]A skilled and rapid response capability to computer viruses, malicious user activity, and vulnerabilities before they can cause significant damage. The phrase "incident response" is used in this report to refer to this capability.

access to sensitive information, are fundamentals of effective policy and oversight of IT security practices.

In 1997 the General Accounting Office (GAO) identified IT security as "a new high-risk area that touches virtually every major aspect of government operations." GAO identified several underlying factors and concluded that some are not technological factors, but "people" factors, such as "insufficient awareness and understanding of information security risks among senior agency officials," "poorly designed and implemented security programs," "limited oversight of agency practices," and "a shortage of personnel with the technical expertise needed to manage controls." Some of these issues are magnified by rapidly changing technology, employee turnover, and inadequate training. Fiscal constraints can also be a limiting factor.

The Computer Security Act of 1987, Public Law 100-235, recognized that improving the security of sensitive information[8] in federal computer systems is in the public interest and required the Department's National Institute of Standards and Technology (NIST) to develop standards and guidelines to ensure cost-effective security. The act also required agencies to establish security plans and required mandatory periodic IT security training. The requirements for IT security are reiterated and expanded in the Government Information Security Reform Act, October 2000. The act recognizes the highly networked nature of federal systems and the need for improved security management measures and effective government-wide oversight. The act specifically requires CIO and Office of Inspector General (OIG) oversight. The Office of management and Budget (OMB) subsequently issued Memorandum 01-08, *Guidance on Implementing the Government Information Security Reform Act*, January 2001. OMB requires CIO and OIG coordination of the oversight efforts.

OMB issued a revised Circular No. A-130, *Management of Federal Information Resources*, February 1996, which replaced a 1985 version. The circular's appendix III, "Security of Federal Automated Information Resources," establishes a minimum set of controls and incorporates requirements of the Computer Security Act. The circular also assigns responsibility to NIST for updating existing guidance and developing new guidance, providing federal agencies with assistance concerning effective controls for systems, assessing security vulnerabilities in new information technologies and informing agencies about the vulnerabilities, and coordinating agency incident response activities. As a result, NIST issued several special publications to supplement the act and Circular A-130.

OMB Circular A-130, Appendix III, is more detailed than the two acts and has two main focuses: general support systems and major applications. General support refers to interconnected

[8]Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, but that has not been specifically designated as classified.

systems that share common functionality. Local area networks and data processing centers that support multiple users are general support systems. OMB assumes that all general support systems contain some sensitive information. The circular focuses extra security controls on a limited number of particularly high-risk major applications. An application involves the use of information resources (information and information technology) to satisfy a specific set of user requirements. An application could be a payroll system that is supported by a network (general support system) to allow remote entry. A major application is one that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in it.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this evaluation was to assess the effectiveness of the CIO's policy and oversight of the Department's IT security program, generally excluding classified systems. We satisfied this objective by evaluating the CIO's compliance with laws and regulations governing IT security, including (1) The Computer Security Act of 1987, (2) OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems," (3) the Government Information Security Reform Act, October 2000, and (4) Department Organization Order 15-23, "Chief Information Officer." Detailed criteria were obtained from the following NIST Special Publications written in response to items 1 and 2:

- 800-04, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials*, March 1992.
- 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.
- 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.
- 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.
- 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

We compared the Department's *Information Technology Management Handbook*, Chapter 10, "Information Technology Security," and attachment, "Information Technology Security Manual," against the criteria to evaluate the CIO's policy. The IT Security Program Manager recognizes the need to update all of the CIO's IT security policy and has drafted one revised section. A completion date for revising the bulk of the policy has not been established. We analyzed the Department's policy early in our review and summarized the results in the nine-page document, *Preliminary Analysis of Commerce CIO IT Security Policy*, October 10, 2000.

We evaluated oversight by reviewing all documents and actions in the last three years related to CIO oversight or management of the Department's IT security program. The review included the CIO's oversight of assessments of operating unit IT security programs based on a recent CIO Council methodology[9], documentation of meetings between the Office of the CIO and operating units about IT security issues, CIO briefings, a draft FY2000/2001 IT Security Management Plan, and minutes of Department of Commerce IT Security Coordinating Committee meetings. We interviewed the Director of the Office of Information Policy, Planning and Review and the IT Security Manager, and participated in a demonstration of an IT Security Systems Database under CIO development.

We held an informal entrance conference with the Director, Office of Information Policy, Planning and Review, and the IT Security Manager on August 23, 2000. Our formal entrance conference was held November 14, 2000. Our field work was conducted from August to December 2000. This evaluation and a concurrent evaluation of the Office of Security's policy and management of classified systems are precursors to systems-level reviews we plan to conduct at the Department's operating units.

[9]The methodology used by the Department was contained in the CIO Council's draft Federal Information Technology Security Assessment Framework. The document was finalized November 28, 2000.

FINDINGS AND RECOMMENDATIONS

The Department's policy and oversight of IT security for sensitive systems needs to be improved. The policy was written before a significant revision to OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, "Security of Federal Automated Information Systems," in 1996. The policy does not comply with the OMB guidance in several areas, and important issue-specific topics are omitted.

In addition to revising and expanding policy, the CIO should implement a compliance review program to ensure the confidentiality, integrity, and availability of the Department's sensitive information. Several factors contributed to the CIO exercising minimal oversight of IT security for several years prior to 1999. A CIO-directed preliminary assessment of operating unit IT security programs in March 2000 determined that substantial improvement was needed. The CIO increased its focus on IT security beginning in 1999 and has made considerable progress in improving compliance. However, continued improvement and additional oversight are needed.

I. The Department's IT Security Policy Needs to Be Revised and Expanded

Department Organization Order (DOO) 10-5, "Chief Financial Officer and Assistant Secretary for Administration," January 14, 1999, Section 2.04, assigns to the Department's CIO responsibility for Department-wide approval and risk management responsibility for automated information systems, including development, coordination, and implementation of policies, plans, and rules, and in collaboration with the Deputy Assistant Secretary for Security, the security of information systems throughout their life cycle. DOO 15-23, "Chief Information Officer," July 3, 2000, Section 4.a, further defines the CIO's responsibility to develop, coordinate, and implement policies and programs for the effective management of the Department's IT resources.

The policy contained in the Department's IT Management Handbook, Chapter 10, "IT Security," and accompanying *IT Security Manual*, is out of date and missing important elements. The policy is out of date because it was developed in 1993 and 1995, prior to a significant revision of OMB Circular A-130. It is missing important components because it has not kept pace with recent trends in technology usage and related security threats. It is important that the Department's policy is current and complete because it is used by the operating units as the foundation of their general policy and to write system-specific policy.

OMB Circular A-130 was revised in February 1996. Most of the Department's policy was written in September 1993, and the main body of policy has not been updated since the circular's revision. Section 10.20, "Electronic Commerce," was issued July 1995. Policy sections on local area network security and copyrighted software were also added in 1995. An e-mail was issued

by the Department's Chief Financial Officer in August 1998 concerning Internet Use Policy, but this policy has not formally been incorporated into the IT management directives system.

The major areas of the Department's policy needing revision address the content of IT security plans,[10] the systems certification process, performing verification reviews[11] of individual systems, reporting security incidents, the form of risk assessments, contingency and disaster recovery planning, security awareness and training, Designated Approving Authority,[12] and referencing related federal IT requirements. Issue-specific policy that needs to be added to the Department's guidance includes Internet usage, e-mail, web security, and communications. These areas are discussed in sections A through J.

A. Security plan criteria should be updated

The security plan criteria referred to in subsection 10.2 of the Department's *IT Management Handbook*, Chapter 10, "IT Security," is outdated. It is based on OMB Bulletin No. 90-08, which was superseded by the revised OMB Circular A-130 and no longer reflects current policy. The revised circular outlines new format and content requirements, including the addition of two important areas: rules of behavior[13] and technical controls.[14]

The revised circular also assigns NIST responsibility for providing agencies with guidance on security planning. To fulfill this responsibility, NIST issued Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998. The

[10]A plan that provides an overview of a system's security requirements and describes the controls in place or planned for meeting those requirements.

[11]System-level reviews to ensure that appropriate protection is being provided based on a system's unique requirements. An overview of the requirements should be documented in the system's IT security plan.

[12]OMB Circular A-130 requires that general support systems and major applications be authorized for processing before use or when established systems undergo significant changes. The Department defines this person as a Designated Approving Authority.

[13]Requirements for use of, security in, and the acceptable level of risk for a system. They delineate responsibilities for those with access to the system and specify limits on interconnections to other systems, service provisions, and restoration priorities. They also specify consequences of behavior not consistent with security policy.

[14]Features that are part of, or can be used by, systems to improve security. They include procedures for identifying and authenticating system users, restricting access to specified information, establishing audit trails and logs, and using cryptography (the process of mathematically scrambling understandable information, rendering it unintelligible, and subsequently restoring it to an intelligible form).

publication includes more detailed guidance on systems analysis; plan development; management,[15] operational,[16] and technical controls for major applications and general support systems; and a format for writing rules of behavior. Although the CIO issued a memorandum in 1999 alerting operating units to the current guidance, the updated policy should be included in a revision to the *IT Management Handbook.*

B. The requirements for certification should be revised

Certification is an in-depth testing of technical controls. Certification in the past has been a requirement for a system accreditation,[17] or authorizing a system for processing. Subsection 10.3 in Chapter 10 assumes that in-depth certification testing of technical controls is necessary to support accreditation. However, according to NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995, Chapter 9, "Assurance," it is now recognized that other analyses, such as risk analysis or audit, can provide sufficient assurance for accreditation and should be considered for lower-risk systems.

OMB Circular A-130 recognizes that management authorization should be based on an assessment of management, operational, and technical controls. Since the security plan establishes the security controls, it should form the basis for the authorization, supplemented by more specific analyses as needed. The circular further states that systems should be re-accredited at least every three years. Performing certifications on the hundreds of Commerce systems requires considerable time and resources and as a result, certifications are not always performed. If alternative procedures were used for accrediting lower-risk systems, such as using information security assessments scheduled to be performed on the Department's critical infrastructure systems,[18] more systems would be certified, while realizing significant savings.

---

[15]Policy, program and system-level management, risk management, and assurance (including accreditation [see the footnote 17 for a definition of accreditation]).

[16]Personnel/user controls; preparation for contingencies and disasters; handling security incidents; awareness, training, and education; systems support; and physical and environmental security.

[17]According to OMB Circular A-130, 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 the risk associated with it.

[18] Systems essential to the minimum operations of the government. Many critical infrastructure systems are subject to accreditation. The CIO in September 2000 arranged for the training of 36 staff representing a variety of operating units in the methodology for conducting information security assessments, and is encouraging operating units to perform self-assessments. The CIO also indicated that funds have been requested by some operating units to contract for assessments.

C. Self-verification reviews should be encouraged

Verification reviews are performed on individual systems based on their unique security requirements to ensure that appropriate levels of protection are being provided. According to subsection 10.5 of the Department's Handbook, these reviews must be performed independent of the system owner. The Department's policy does not distinguish between verification reviews for general support systems and major applications. Circular A-130, however, encourages self-verification reviews for lower risk systems.

For general support systems, reviews should ensure that management, operational, and technical controls are functioning effectively. Security controls may be reviewed by an independent audit or a self-review. The type and rigor of review should be commensurate with the acceptable level of risk that is established in the rules of behavior for the system and the likelihood of learning useful information to improve security during a review. For example, a general support system used in conjunction with a major application would typically be subject to a more rigorous review than a local area network supporting office automation. Circular A-130 recommends independent reviews for major applications because of their higher risk.

Technical tools, such as virus scanners, vulnerability assessment products, and penetration testing, can assist in the ongoing review of different facets of systems. However, these tools are no substitute for a formal management review at least every three years. For some high-risk systems with rapidly changing technology, more frequent reviews may be necessary. Self-reviews would reduce the need for the Department to assemble and oversee independent review teams and could result in increased coverage and significant resource savings.

D. IT security incidents should be reported to the OIG

The Department's current policy specifies that IT security incidents[19] should be reported to the IT Security Manager. The policy should also require operating units to notify the OIG because of the responsibilities specified in the Inspector General Act, as amended, and Departmental Administrative Order 207-10 for keeping abreast of significant issues in the Department.

The Department's policy on handling security incidents is contained in section 6.1, "Malicious Software," of the IT Security Manual, and was reinforced in a July 8, 1999, memorandum from the Department's CIO to the operating unit CIOs. The policy calls for operating units to notify

[19] A compromise of integrity, such as when a virus infects a program or a serious system vulnerability is discovered; denial of service, such as when an attacker has disabled a system or a network worm has saturated network bandwidth; misuse, such as when an intruder (or insider) makes unauthorized use of an account; damage, such as when a virus destroys data; and intrusions, such as when an intruder penetrates system security.

the IT Security Manager within 24 hours and submit a structured written report as soon as possible after the occurrence of an incident. Through informal means, the OIG has been notified of some incidents, but reporting has been inconsistent.

Unless the requirement to notify the OIG of security incidents is specifically identified in the Department's policy, agencies may not know about the requirement. The Inspector General Act of 1978, as amended, requires the Inspector General to keep the Secretary and the Congress fully and currently informed about problems and deficiencies relating to the administration of Department of Commerce programs and operations and the necessity for and progress of corrective action, and to report potential federal crimes to the Attorney General. In some cases, operating units notify the Attorney General directly, cutting the OIG out of the information loop. According to Department Administrative Order 207-10, operating units must promptly report to the OIG the possible existence of violations of laws, rules, or regulations.

While reviewing the CIO's files of written incident reports from operating units, we observed that the vast majority were for unsuccessful access attempts that were of no consequence to the operating unit. In other words, the reported events 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, but rather, were minor nuisances. Under these circumstances, the Department may want to 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 even repeated access attempts by the same address. Statistics on failed attempts could be kept by operating units and reported centrally periodically. The revision of reporting requirements would ease the burden of central reporting on the operating units and the Office of the CIO.

E. Risk assessment policy should be reconsidered

The Department's policy requires documented risk assessments[20] to ensure that the balance of vulnerabilities, threats, and safeguards achieves a residual level of risk that is acceptable based on the sensitivity or criticality of the individual system. The analyses may vary from informal but documented reviews for smaller, lower risk systems, to fully quantified risk analyses for systems that are larger and contain more risk. The revised circular, however, no longer requires the preparation of formal risk analyses, not even for larger, more complex systems.

[20]The process of analyzing and interpreting risk. The terms "vulnerability analysis" or "vulnerability assessment" are sometimes used synonymously with risk assessment. However, vulnerability analysis/assessment is just one component of risk assessment. When assessing risk to an asset, vulnerability must be considered along with threats and safeguards.

OMB recognizes that "in the past, substantial resources have been expended doing complex analyses of specific risks to systems, with limited tangible benefit in terms of improved security for the systems." OMB's risk-based approach to IT security now recognizes that "security efforts are better served by generally assessing risks and taking actions to manage them." Additional guidance on performing assessments is contained in NIST's Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook,* Chapter 7, "Computer Security Risk Management," October 1995.

Related to risk analysis, and required by Presidential Decision Directive 63 to provide security for the nation's critical infrastructure, are vulnerability assessments. The Department's universe of critical infrastructure assets in many cases overlap the Department's classified and sensitive computer systems inventory. The analysis of vulnerabilities along with threats and safeguards is an integral part of analyzing the risk to assets. Because of the interrelationship of the two assessments and the similarity in the Department's universes of critical infrastructure assets and sensitive IT systems, the CIO intends to link the assessments. This linkage should be made in its IT security policy also. Combining the assessments could improve efficiency while also improving operating unit compliance.

F. Contingency and disaster recovery back-up planning should be reemphasized

Chapter 10, Section 10.8, "Contingency and Disaster Recovery Planning," provides good policy concerning backup and retention of data and software, emergency response actions, and resumption of normal operations. The policy also requires selection of a backup or alternate operations strategy. However, the policy does not state whether manual procedures are a viable backup option.

The revised OMB circular states that manual processing is generally *not* a viable backup option for general support systems and major applications. Manual operations may be acceptable for operations where volume is low and there is assurance that automated operations can be resumed in a relatively short time frame. However, the lack of specific policy on backup options may create a false sense of security for continuity of important departmental operations. Information technology has become more vital to the continuity of government operations as automation investments have increased. The lack of automated support for some of the Department's functions could cease or significantly impair operations. The OMB guidance on manual backup, therefore, should be included in the Department's revised policy.

G. Mandatory pre-access training should be highlighted

The Department's current policy states that all new employees will receive an IT security awareness briefing as part of their orientation within 60 days of their appointment, and be

provided with refresher security awareness material or briefings at least annually. OMB Circular A-130, however, requires that employees be trained on how to fulfill their security responsibilities *before* being allowed access to sensitive systems. Failure to make individuals with access to systems aware of their security responsibilities increases security risk.

For general support systems, employees involved in the management, use, or operation of federal computer systems within or under the supervision of the federal agency, including contractors, need training on how to fulfill their security responsibilities, including the rules of behavior, before access is permitted. Access provided to the public should be constrained by controls in the application through which access is allowed, and training should be within the context of those controls. Training should also inform users on how to get help in the event of difficulty with using or securing the system. Training may vary from interactive computer sessions or well-written and understandable brochures to formal classroom training depending on the amount of system risk.

For major applications, individuals with access should receive specialized training focused on their responsibilities and the application rules of behavior. The specialized training may be in addition to the training required for access to the system. According to the circular, "this training could vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application)."

H. Designated Approving Authority for nonclassified systems should be a management official

The Department's policy establishes the operating unit CIOs as the Designated Approving Authority for accrediting all sensitive IT systems within the Department. The authority at the operating unit level can only be delegated to a senior management official if that official does not have direct control over the IT system being accredited. This policy is contrary to OMB Circular A-130, B. "Descriptive Information," a.4, which states that authorization is not a decision that should be made by security staff, but rather normally by the person having general responsibility for the organization supported by the system.

The circular states that general support systems should be accredited in writing by the management official based on implementation of the system's security plan before beginning or significantly changing processing in the system. The circular further requires that the system be re-authorized at least every three years. Since the security plan establishes the security controls, it should form the basis of the accreditation. The circular specifically prohibits security staff from making the decision.

Similarly, major applications should be accredited by the management official responsible for the function supported by the application. The intent of the requirement is to ensure that the senior official whose mission will be adversely affected by security weaknesses in the application periodically assesses and accepts the risk of operating the application. Accreditations of major applications should take into consideration the risks from the general support systems used by the application. NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995, Chapter 9, "Assurance," section 9.1, supports the circular by stating that "accreditation is a management official's formal acceptance of the adequacy of a system's security."

The OMB criteria encourage participation of IT security professionals and management officials in a collaborative effort. We believe that OMB has highlighted the importance of management involvement because, in the past, managers have not always taken an active role in understanding the risks of and establishing controls over the sensitive information they are responsible for. To ensure this involvement, the CIO should take an active role in ensuring that accreditations are properly performed, but senior managers should decide the level of risk for the systems.

I. Related federal requirements should be added

A broad spectrum of federal criteria must be understood to effectively manage IT resources. There are several that are closely interrelated to IT security and should be included in the Department's policy. For example, there is no provision in the policy for reporting IT security deficiencies as material weaknesses pursuant to OMB Circular A-123, *Management Accountability and Control*, and the Federal Manager's Financial Integrity Act (FMFIA). Failure to report significant IT security weaknesses could result in a lack of management attention to unacceptably high security risks. The policy also does not require that a summary of agency security plans be included in the information resources management plan that is sent to OMB.

Circular A-130 requires a review of security controls in each system when significant modifications are made to the system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the systems as determined during accreditation. Circular A-130 asks operating units to identify security deficiencies pursuant to Circular A-123 and FMFIA if during the reviews it is determined that there is no assignment of security responsibility, no security plan, or no accreditation. The operating unit's determination to report a material weakness should depend on the risk and magnitude of harm that could result from the weakness.

The requirement that a summary of agency security plans be included in the information resources management plan is contained in the Computer Security Act of 1987. To ensure that

the plan summaries could not be used to attack the Department's sensitive or classified systems, specific vulnerabilities should not be revealed there.

There are several other federal policies that should be included and logically linked to IT security, including OMB Memorandum 00-07, *Incorporating and Funding Security in Information Systems Investments*, February 2000; the Clinger-Cohen Act,1996, which links security to agency capital planning and budget processes; Presidential Decision Directive 63, *Protecting America's Critical Infrastructures*, 1998, which specifies agency responsibilities for protecting the nation's infrastructure and assessing and eliminating vulnerabilities. The new Government Information Security Reform Act makes reference to additional criteria, including the Chief Financial Officers Act of 1990, Government Performance and Results Act,1993, and the Federal Financial Management Improvement Act, 1996.

J. Issue-specific policy concerning Internet usage, e-mail, web security, and communications should be added

The Department's policy does not include relevant issue-specific security guidance for topics such as Internet usage, e-mail, web security, and communications. The Department issued policy in April 1992 through Departmental Notice Series 92-3, "Establishment of Departmental Policy for E-Mail Privacy," but the policy addresses security only to the extent of transferring information about an individual in electronic form.

More comprehensive guidance was issued in August 1998 in an e-mail from the Department's Chief Financial Officer and Assistant Secretary for Administration concerning Internet use policy. The Internet policy links precautions on the transfer of information using the Internet and e-mail to the security standards used to certify and accredit the Department's systems. This policy should be incorporated into the Department's IT security policy and linked to communications, cryptography, and digital signatures as appropriate. Policy concerning web security and communications security should be developed and linked in a similar manner.

Issue-specific policy should address current relevant concerns to the organization. This policy should be updated more frequently than general program policy as changes in technology and security threats occur. The policy should contain an issue statement that explains the CIO's position, applicability, roles and responsibilities, compliance, and points of contact. Operating units should be given responsibility for translating the issue-specific policy into system-specific policy based on particular system security objectives and rules of behavior specified in IT security plans. For example, the system-specific policy should indicate which data or records can and cannot be transferred via e-mail or the Internet and state whether security controls such as cryptography apply to the transfer of specified information.

Complete and up-to-date issue-specific policy is important because, along with program-level policy, it forms the basis for operating unit policy. Specific guidance on the formulation of issue-specific policy is contained in NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995, Chapter 5, "Computer Security Policy, " and NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996, section 3.1, "Policy."

K. Recommendation

We recommend that the CIO revise the outdated program policy and incomplete issue-specific policy for the Department's IT security program as soon as possible. The revised policy should include:

1. Current federal criteria for the format and content of IT security plans, as specified in NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

2. A provision for alternatives to formal certifications for lower risk systems, such as risk analyses or audits.

3. A provision for self-verification reviews for general support systems with lower risk.

4. A requirement to notify the OIG in the event of IT security incidents involving the Department's systems, networks, or web sites or any other IT security matter that involves the manipulation, destruction, or loss of data or systems, or denial of service including repeated penetration attempts from the same Internet address.

5. A change in risk assessment emphasis from complex, documented assessments that focus on specific risks to general risk assessments. Also, risk assessments should be linked in policy and practice to vulnerability assessments required under Presidential Decision Directive 63.

6. Guidance to operating units that manual operations are generally not a viable backup option for the Department's systems.

7. A requirement that individuals be trained on how to fulfill their security responsibilities before they are permitted access to sensitive systems.

8. A change in the Designated Approving Authority for sensitive systems from the CIO to a management official having responsibility for the function supported by the system.

9. A requirement for operating units to include IT security deficiencies as material weaknesses pursuant to OMB Circular A-123 and FMFIA, and to include in their information resources management plans summaries of agency IT security plans pursuant to the Computer Security Act of 1987. Links should also be added to other federal IT security-related criteria, such as OMB Memorandum 00-07, the Clinger-Cohen Act, *Presidential Decision Directive 63*, the Government Performance and Results Act, the Chief Financial Officer's Act, and the Federal Financial Management Improvement Act.

10. Issue-specific IT security policy on Internet usage, e-mail, web security, and communications.

L. CIO response and OIG comments

The CIO agreed with our recommendation to revise and expand the Department's IT security policy and plans to update the policy in the immediate future. However, while the CIO stated that the office followed OMB's model of updating policy only at significant intervals by issuing memorandums, we reaffirm our position that the major revision to OMB Circular A-130 in 1996 constituted the point where the Department's policy should have been updated. A current, comprehensive, and cohesive IT security policy is the foundation for a sound IT security program. We recognize that the CIO has significantly improved the Department's IT security program over the past two years, but the program stills lacks adequate staff to perform its critical functions.

The CIO disagreed with or asked for further clarification of several statements used to support our recommendations. First, the CIO disagreed with an example we provided to accredit lower-risk systems based on IT security assessments scheduled to be performed on the Department's critical infrastructure systems. The CIO stated that the Administration had not provided adequate priority and funding to the critical infrastructure program. We agree that the lack of funding significantly affected critical infrastructure program activities. However, in September 2000, the CIO arranged for the training of 36 staff representing a variety of operating units in the methodology for conducting IT security assessments and has encouraged operating units to perform self-assessments. We believe these assessments can contribute to fulfilling accreditation requirements.

Second, although the recommendation to notify the OIG in the event of an IT security incident involving the Department's systems, networks, or web sites was accepted, the CIO requested that

the OIG provide specific guidance as to when notification is required. We agree that specific guidance is needed, and we will work with the CIO to define the notification guidance.

Third, the CIO asked for a clarification of our use of terms specific risks and general risks. Our source for these terms is Appendix III of OMB's Circular A-130, and we referenced NIST's Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, Chapter 7, "Computer Security Risk Management," October 1995, as additional guidance for performing risk assessments. The intent of OMB Circular A-130 was to change the method used to evaluate security risks from a formal and infrequent assessment, called analyzing specific risks, to a more robust assessment that continually assesses new threats, vulnerabilities to system software, and vulnerabilities to application software, called generally assessing risks.

Fourth, the CIO agreed with our recommendation to report security deficiencies as material weaknesses when there is no assignment of security responsibility, no security plan, or no accreditation, but expressed concerns about the ability to implement this recommendation. We believe, however, that the CIO, along with the operating units, should identify the most critical departmental systems, define a reporting strategy, and specify interim milestones.

Finally, the CIO stated that operating units are already required to report on their strategies to address IT security in their annual plans and does not understand the deficiency. The Department's IT security policy does not specify this reporting requirement and therefore should be updated to formally establish the requirement.

The CIO's complete response is included as Appendix B.

II. CIO Has Taken Steps to Improve IT Security, But Additional Efforts Are Needed

As described in the previous section, the Department's IT security program is not fully in compliance with OMB Circular A-130. Although the CIO has considerably improved IT security compliance recently, for several years there was minimal oversight. As a result, for many systems valid IT security plans are not in place, and accreditation and verification reviews have not been performed. In addition, several operating units do not have adequate awareness/training programs or incident response capabilities.

We commend the CIO for initiating several actions to bring the Department in compliance with current federal IT security policy. In 1999 the CIO contracted for an evaluation of the Department's critical infrastructure protection plans and related IT systems security plans. The CIO also issued a June 1999 memorandum calling for operating units to prepare plans and schedules by July 1999 to address the elements of the IT security program outlined in the

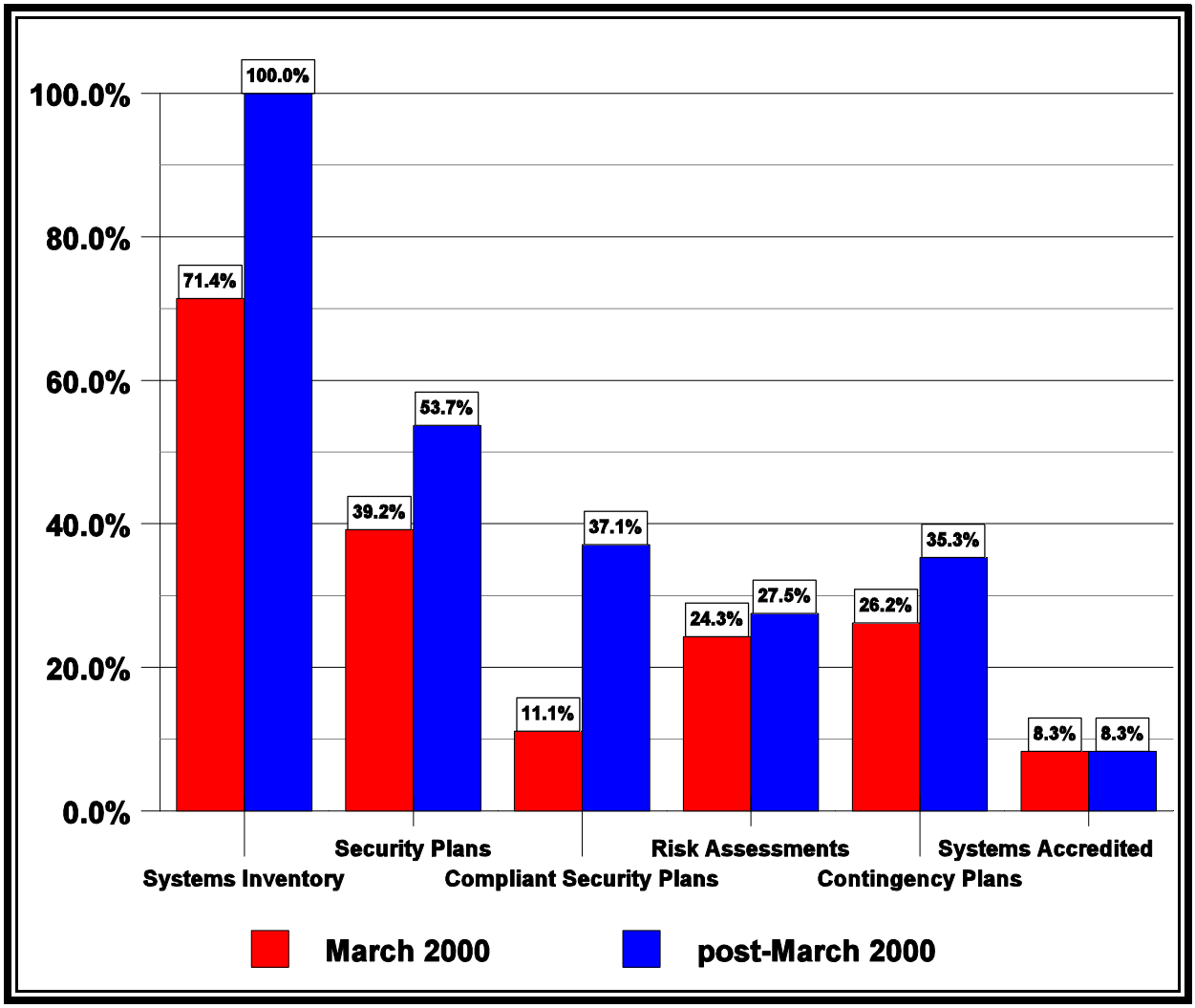
Department's *IT Management Handbook*, Chapter 10, "IT Security." The memorandum called for submitting new IT security plans for all systems identified by the contractor as having non-existent or out-of-date plans and to bring all plans into compliance with NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

In addition, the CIO used a draft Federal Information Security Assessment Framework from the Federal Chief Information Officers Council to determine the status of operating unit IT security programs by issuing a data call in March 2000. The data call asked operating units about systems inventories, the existence and compliance of IT security plans, risk assessments, contingency plans, accreditations, awareness and training programs, and incident response capabilities. The CIO then summarized the results and held meetings with the political head of each unit when available, the ranking career executive, the operating unit CIO, and the operating unit IT Security Officer. The purpose of the summary status and meetings was to give operating units advance notice of the assessment criteria that will be adopted by the Department, and to provide the units with an assessment of the strengths and weaknesses of their IT security programs.

The March data call revealed that the Department's IT security program needed attention. The results showed that the systems inventory was not complete and that overall IT security program compliance was minimal. In addition, IT security awareness/training programs and incident response capabilities were absent or informal. However, follow-up reviews conducted prior to each meeting showed significant improvement in operating unit compliance as a result of the CIO's initiative. The results of the March 2000 and follow-up status are summarized for the Department as a whole in Figure 1.

We believe the lack of oversight of IT security in the operating units largely contributed to the non-compliance status observed in March 2000. The Department's IT Security Manager position was vacant for a year prior to June 1997. Until March 2000, only one person handled the function, performing all policy, management, and administrative duties. In March, the position was upgraded, and the function was expanded to four full-time equivalent personnel. However, the group's most experienced staff member recently left for another position. Staffing and training are priorities for the CIO's IT security group. Funding for IT security has also been a problem. There is no central budget for the CIO's IT security work except for salaries and limited available funding must compete with other CIO activities

Figure 1. Department of Commerce Information Technology Security Program Status



There is an initiative that is intended to improve the authority of operating unit CIOs and better focus IT security oversight and funding. The CIO is proposing a restructuring of the Department's information technology organization. The restructuring would, among other things, allow the Department's CIO to establish and evaluate 50 percent of the performance plans for operating unit CIOs and improve performance plans and accountability for all managers and

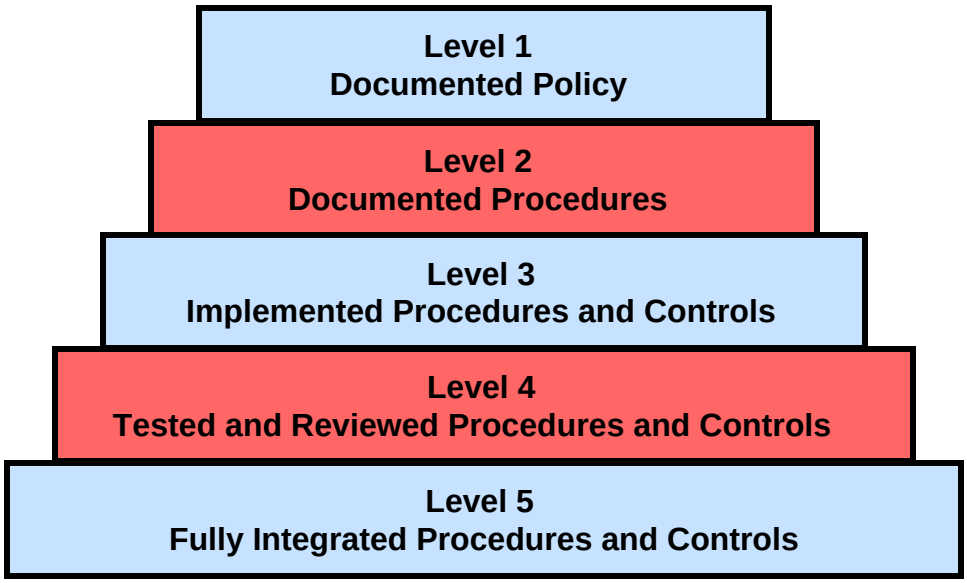
employees who perform IT work. The restructuring is also intended to increase the involvement of operating unit CIOs in budgeting for IT resources.

The Department's inventory of systems is complete, although a final number will not be available until IT security plans covering multiple systems are tallied. An accurate inventory of the Department's sensitive systems is important in identifying all systems that should be subject to IT security and covered by IT security plans. The presence and quality of IT security plans are an important indicator of the quality of an operating unit's IT security program. IT security plans contain an overview of a system's security requirements, including rules that delineate responsibilities and expected behavior of all individuals with access to the system, as well as training needs, personnel controls, incident response capability, contingency plans, technical security controls, and system interconnection. Without current plans, there is no assurance that the security of systems containing sensitive information has been fully considered. Risk assessments are important because they identify the threats and vulnerabilities to systems. Contingency plans are needed to determine the viability of back-up procedures for continuing operations. The accreditation process ensures that risk is considered by management before a system is initially commissioned or after it is significantly modified.

The CIO had tentative plans to develop and manage a compliance review program but was not sure of the scope of the oversight and was concerned about whether sufficient resources and funding were available. In October 2000, the Government Information Security Reform Act was signed into law, making it mandatory for the CIO and the Office of Inspector General to conduct annual reviews of IT security in FY 2001 and 2002. OMB issued Memorandum 01-08, *Guidance On Implementing the Government Information Security Reform Act*, dated January 16, 2001, which endorses the CIO's use of the CIO Council Framework as the basis for the annual program review. The framework helps agencies to determine the status of their security programs and employs five levels as shown in Figure 2. The framework will employ a self-assessment questionnaire that will be completed by NIST in 2001. The framework begins with the premise that all agency assets must meet the minimum security requirements of Circular A-130 and results in a compliance level rating for the operating unit.

The OIG responsibilities under the act according to OMB include an evaluation in FY 2001 and 2002 of the Department's security program and practices. This includes testing the effectiveness of security controls for "an appropriate subset of agency systems." OIGs should use the results of security-related evaluations performed by other experts, including the agency program reviews performed under the CIO Framework methodology. The CIO and the OIG are encouraged to work closely when developing their work plans to avoid unnecessary duplication and overlap. In accordance with OMB guidance, the OIG will conduct reviews at selected operating units focusing on system-level policy and procedures. These reviews will include testing technical

Figure 2. Federal IT Security Assessment Framework



controls. DOO 15-23, "Chief Information Officer," July 3, 2000, Section 3.01.c, defines the CIO's responsibility for implementing OMB Circular A-130 and for developing and implementing a Department of Commerce IT security program to ensure the confidentiality, integrity, and availability of information and IT resources, including the review of IT security, in coordination with the Deputy Assistant Secretary for Security. Section 4.a further defines the CIO's responsibility to develop, coordinate, and implement programs for the effective management and evaluation of the Department's IT resources.

The Government Information Security Reform Act and DOO 15-23 require the CIO to exercise broad program responsibility for IT security in the Department. In addition to overseeing the CIO Council Framework self-assessments, the CIO should commit to a program of operating unit reviews that extends beyond the two-year review requirement of the act. The reviews should determine that operating unit program-level and issue-specific policy is in compliance with federal IT security policy and the Department's revised program-level policy, that each unit has IT security awareness and training programs, and that each unit implements a formal incident response capability.

To ensure that IT security is planned and funded in future IT acquisitions, the CIO should work with the Department's Office of Acquisition Management and the Office of Budget to ensure that

IT-related procurement specifications for hardware, software or services include adequate security requirements and specifications that are commensurate with the sensitivity of the system, and that security requirements are included in operating unit budgets. The CIO should also notify operating unit heads and CIOs about the requirement to report deficiencies in IT security as material weaknesses pursuant to OMB Circular A-123 and FMFIA, as discussed on page13 of this report.

The CIO's program should employ sampling techniques and include review of IT security plans for the most critical Commerce systems to determine whether they comply with NIST Special Publication 800-18. Reviews should also include sampling of operating unit IT security documents to ensure that (1) the accreditation process is functioning properly and that accreditation status reports are accurate, (2) the security controls in each system are reviewed at least every three years or when significant modifications are made to a system, and (3) operating unit systems are audited periodically for illegal software or that some other mechanism exists for ensuring that only legal copies of software are being used. Our office will coordinate with the CIO to ensure that there is no duplication in the systems-level oversight.

A. Recommendation

In addition to the oversight of operating unit self-assessments using the CIO Council Framework, we recommend that the CIO commit to an operating unit compliance review program that extends beyond the FY 2001 and 2002 requirement of the recent Government Information Security Reform Act. Reviews should begin as soon as possible and should ensure that operating units:

1. Have program-level, issue-specific, and system-level policy in place that complies with federal IT security policy and the Department's revised program-level policy.

2. Implement formal IT security awareness and training programs.

3. Develop incident response capabilities.

4. Report deficiencies in IT security as material weaknesses pursuant to OMB Circular A-123 and FMFIA.

5. Include IT-related procurement specifications for hardware, software or services, to ensure that they include adequate security requirements and/or specifications that are commensurate with the sensitivity of the system, and that security requirements are included in operating unit budgets. The CIO should work with the Department's Office of Acquisition Management and the Office of Budget to ensure implementation.

6. We also recommend that the review program include procedures to review on a sample basis operating unit IT security documents to determine that:

   a. IT security plans are prepared for all sensitive systems and that they comply with NIST SP 800-18.

   b. Systems are accredited and that a management official was involved in the accreditation process.

   c. Verification reviews of individual systems are conducted at least every three years or when significant modifications are made to systems and that the scope of the reviews is appropriate based on system risk.

   d. Systems are audited periodically for illegal software or that some other mechanism exists for ensuring that only legal copies of software are being used.

B. CIO response and OIG comments

The CIO agreed to continue the IT security compliance review program beyond the FY 2002 duration of the Government Information Security Reform Act, to begin security reviews as soon as possible, and to make specific security improvements at the operating unit level. However, the response notes that limited staff resources will prevent the CIO from performing hands-on compliance review of operating units to fulfill OMB reporting requirements for FY 2001. To meet the FY 2001 reporting requirements, operating units will perform a self-assessment of their IT security using the Federal CIO Council's Security Assessment Framework. Following the FY 2001 review, the CIO will evaluate the results of the self-assessment approach to aid in the planning of future security reviews.

We address the approach to reporting security deficiencies as a material weakness in our previous comments on the CIO's response to our first finding.

The CIO's complete response is included as Appendix B.

APPENDIX A
3 Pages

Glossary of IT Security Terms

Accreditation - According to OMB Circular A-130, accreditation is the authorization of a system to process information granted by a management official. By authorizing processing in a system, a manager accepts the risk associated with it.

Classified Information - Information that requires protection against unauthorized disclosure and is marked to indicate its classified status pursuant to Executive Order 12958. Classified information is generally afforded more security than sensitive information.

Certification - An in-depth testing of technical controls. Certification is used to support accreditation.

Critical Infrastructure - Systems essential to the minimum operations of the government. In many cases, the Department's sensitive and classified information systems are also considered critical infrastructure.

Designated Approving Authority - OMB Circular A-130 requires that general support systems and major applications are authorized for processing before use or when established systems undergo significant changes. The Department defines the person responsible for authorization as a Designated Approving Authority. According to the Department's IT security policy, the Designated Approving Authority is responsible for ensuring appropriate and adequate levels of protection for all IT systems.

Firewall - A device that protects a private network from the public part. Usually, a computer is set up to monitor traffic between an Internet site and the Internet. It's designed to keep unauthorized outsiders from tampering with a computer system therefore increasing security.

General Support Systems - Interconnected systems that share common functionality. Local area networks and data processing centers that support multiple users are general support systems. OMB assumes that all general support systems contain some sensitive information.

Hacker - A "hacker" was originally someone who "hacks" around with computers and electronics to understand how things work, but over time, this term has been widely accepted as describing someone who breaks into computer systems. Technically, however, "cracker" is a more accurate term for someone who breaks into computer systems with malicious intent.

Incident Response Capability - NIST refers to this as a Computer Security Incident Response Capability and defines it to be a skilled and rapid response capability to computer viruses, malicious user activity, and vulnerabilities associated with high technology before they can cause significant damage. Various other terminology is associated with this capability, including Computer Incident Response Team, Computer Emergency Response Team, and Computer Incident Response Capability.

Issue-Specific Policy - This level supports program-level policy and is used to address specific issues or topics of concern, such as e-mail security. Section 6.1, "Malicious Software," in the Department's *IT Security Manual* is an example of issue-specific policy.

IT Security Incidents - A compromise of integrity, such as when a virus infects a computer program or a serious system vulnerability is discovered; denial of service, such as when an attacker has disabled a system or a network worm has saturated network bandwidth; misuse, such as when an intruder (or insider) makes unauthorized use of an account; damage, such as when a virus destroys data; and intrusions, such as when an intruder penetrates system security. This phrase is used in this report when referring to Incident Response Capability, defined above.

IT Security Plan - A plan that provides an overview of security requirements of a system and describes the controls in place or planned for meeting those requirements.

Major Application - "Application" refers to the use of information resources (information and information technology) to satisfy a specific set of user requirements. An application could be a payroll system that is supported by a network (general support system) to allow remote entry. A major application is one that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in it.

Management Controls - Policy, program-, and system-level management, risk management, and assurance (including accreditation).

Operational Controls - Personnel/user controls; preparation for contingencies and disasters; handling security incidents; awareness, training, and education; systems support; and physical and environmental security.

Program-Level Policy - High-level policy used to create an organization's computer security program. The Department's *Information Technology Management Handbook*, Chapter 10, "Information Technology Security," is an example of program-level policy.

Risk Assessment - The process of analyzing and interpreting risk. Assessing the risk of an asset includes considering vulnerabilities, threats, and safeguards.

Rules of Behavior - Requirements for use of, security in, and the acceptable level of risk for a system. They delineate responsibilities for those with access to the system and specify limits on interconnections to other systems, service provisions, and restoration priorities. They also specify consequences of behavior not consistent with security policy. Rules of behavior are included in IT security plans.

Sensitive Information - Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, but that has not been specifically designated with the generally more stringent "classified information" status. All general support systems are assumed to contain sensitive information.

System-Specific Policy - Written by operating units for single systems, system-specific policy is often implemented through the use of access controls and supports program-level and issue-specific policy.

Technical Controls - Features that are part of, or can be used by, systems to improve security. They include procedures for identifying and authenticating system users, restricting access to specified information, establishing audit trails and logs, and using cryptography (the process of mathematically scrambling understandable information, rendering it unintelligible, and subsequently restoring it to an intelligible form).

Verification Reviews - System-level reviews to ensure that appropriate protection is being provided based on a system's unique requirements. The requirements should be documented in the system's IT security plan.

Vulnerability Analysis/Assessment - A component of risk assessment. When assessing risk to an asset, vulnerability must be considered along with threats and safeguards.

UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

MAR 30 2001

Appendix B

MEMORANDUM FOR: Judith J. Gordon
Assistant Inspector General for Systems Evaluation
Office of the Inspector General

FROM: Roger W. Baker
Chief Information Officer

SUBJECT: *Additional Focus Needed on Information Technology Security Policy and Oversight*, Draft Inspection Report
No. OSE-13573/February 2001

Thank you for your recently completed review of our Information Technology Security Program efforts to date. Once again, my staff found it a pleasure to work with yours in this cooperative effort. As in our previous endeavors, we found your staff to be professional and knowledgeable, and the results to be thorough, helpful, and enlightening. We look forward to continuing our partnership in improving the security of Commerce's information technology resources.

Generally, we agree with your findings and most of our comments reflect how we plan to implement your recommendations. There are several areas where we feel additional guidance from your office would assist us in carrying out the improvements, and several where we are dependent on funding for IT security.

The attached table addresses each finding and recommendation in detail. If you have any questions, please contact the Department's Information Technology Security Manager, Michael Lombard. He can be reached on (202) 482-0277, or by e-mail at mlombard@doc.gov.

Attachment

cc: Lisa Westerback
Mike Lombard
Alan Crawley

Additional Focus Needed on Information Technology Security Policy and Oversight
Draft Inspection Report No. OSE-13573/February 2001

Draft Comments on Recommendations

March 29, 2001

OIG Recommendation	OCIO Comment
I. The Department's IT Security Policy Needs to Be Revised and Expanded	It has been OMB's practice to issue major updates to policy only at significant intervals, and in between, issue memoranda to update or modify policy, as necessary. While we agree that it is time for Commerce to update its IT security policies, we feel that it is important to note that we have followed the same basic principle as OMB, in that we have issued updates and addressed new issues in the form of memoranda.
We recommend that the CIO revise the outdated program policy and incomplete issue-specific policy for the Department's IT security program as soon as possible. The revised policy should include:	We have recently received the authority to fill the vacancy on the IT Security staff, and the position is open as of this writing. It will, therefore, be feasible to begin updating the policy in the immediate future.
1. Current federal criteria for the format and content of IT security plans, as specified in NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.	Our current policy, per the DOC CIO's memorandum to operating unit heads of June 9, 1999, requires that security plans follow NIST SP 800-18. The next revision of the security policy in the IT Management Handbook will incorporate provisions of this memo.
2. A provision for alternatives to formal certifications for lower risk systems, such as risk analyses or audits.	We agree in part. The Department's revised policy will require certification efforts commensurate with the criticality of the system. However, it is imperative to consider interconnections to systems of higher risk, and we plan to require this element in any certification process, even for systems of apparent lesser risk. Given the lack of priority and funding by the Clinton Administration

Additional Focus Needed on Information Technology Security Policy and Oversight **Draft Inspection Report No. OSE-13573/February 2001** **Draft Comments on Recommendations** March 29, 2001	
OIG Recommendation	OCIO Comment
	in the area of critical infrastructure protection, we must disagree with the OIG assertion that using information security assessments scheduled to be performed on the Department's critical infrastructure systems would result in more systems being certified, while realizing significant savings. In the event that the Bush Administration raises the priority of critical infrastructure protection through the application of funding, we will take advantage of assessments gained through this avenue.
3. A provision for self-verification reviews for general support systems with lower risk.	We agree. The Department's revised policy will require verification reviews commensurate with the criticality of the system, with the requirement to consider interconnections to systems of higher risk.
4. A requirement to notify the OIG in the event of IT security incidents involving the Department's systems, networks, or web sites or any other IT security matter that involves the manipulation, destruction, or loss of data or systems, or denial of service including repeated penetration attempts from the same Internet address.	We agree and will take action to ensure that it is carried out. However, there is still a large degree of latitude, which we believe will continue to cause misunderstandings in the future, especially in the area of thresholds for denial of service and repeated attempts. We believe that further discussion is necessary to come to a reasonable understanding. We expect the operating units to have a wide range of opinions as to what that threshold should be and consensus will be a challenge. We would appreciate more specific guidance in this area.
5. A change in risk assessment emphasis from complex, documented assessments that focus on specific risks to general risk assessments. Also, risk assessments should be	We agree in part. The Department's revised policy will require risk assessments commensurate with the criticality of the system. However, we do not understand your distinction between specific

Additional Focus Needed on Information Technology Security Policy and Oversight **Draft Inspection Report No. OSE-13573/February 2001** **Draft Comments on Recommendations** March 29, 2001	
OIG Recommendation	OCIO Comment
linked in policy and practice to vulnerability assessments required under Presidential Decision Directive 63.	risks and general risks, and would appreciate a clarification. Efforts required by PDD-63 are not separate, but rather a prioritization under the overall IT Security Program. The Department's revised policy will reflect that.
6. Guidance to operating units that manual operations are generally not a viable backup option for the Department's systems.	We agree. The Department's revised policy will discourage manual operations, and will specify the conditions of low volume and an assurance that automated operations can be resumed in a relatively short time frame.
7. A requirement that individuals be trained on how to fulfill their security responsibilities before they are permitted access to sensitive systems.	We agree and will update Departmental policy accordingly. The following was proposed, in part, as an element in the CIO performance plans: Require a computer security awareness briefing for new employees before they are allowed access to your IT systems.
8. A change in the Designated Approving Authority for sensitive systems from the CIO to a management official having responsibility for the function supported by the system.	We agree. We propose a change in Departmental policy that would require the certification process to be done in coordination with the operating unit CIO, then have the OU CIO present the risks in an executive-level fashion to the program official, to ensure that they can be understood in a business context, and in a language appropriate to the position and technical understanding of the program official. The program official would then approve the system for processing, or require additional risk mitigation, as appropriate.

Additional Focus Needed on Information Technology Security Policy and Oversight
Draft Inspection Report No. OSE-13573/February 2001

Draft Comments on Recommendations

March 29, 2001

OIG Recommendation	OCIO Comment
9. A requirement for operating units to include IT security deficiencies as material weaknesses pursuant to OMB Circular A-123 and FMFIA, and to include in their information resources management plans summaries of agency IT security plans pursuant to the Computer Security Act of 1987. Links should also be added to other federal IT security-related criteria, such as OMB Memorandum 00-07, the Clinger-Cohen Act, *Presidential Decision Directive 63*, the Government Performance and Results Act, the Chief Financial Officer's Act, and the Federal Financial Management Improvement Act.	In principle, we agree with your recommendation to report security deficiencies as material weaknesses when there is no assignment of security responsibility, no security plan, or no accreditation. However, in practice, we would be reporting 91.7 % of the Department's IT systems. We suggest a two-part alternative: 1. That such reporting begin after a reasonable period of notice and time to comply. We propose one year, and 2. The use of a senior management council as a forum for assessing and monitoring deficiencies in management controls. This is suggested in OMB Circular A-123, and would provide Commerce with a means of determining the risk within each instance of deficiency, and with the means to declare a lesser deficiency that could be handled within the Department. This council could recommend to the Secretary which deficiencies are deemed to be material to Commerce as a whole, and should therefore be included in the annual Integrity Act report to the President and the Congress. This council could also be used to determine when sufficient action has been taken to declare that a deficiency has been corrected. We would invite the

Additional Focus Needed on Information Technology Security Policy and Oversight **Draft Inspection Report No. OSE-13573/February 2001** **Draft Comments on Recommendations** March 29, 2001	
OIG Recommendation	OCIO Comment
	OIG to attend and give counsel at these discussions. In regard to your recommendation that operating units include in their information resources management plans summaries of agency IT security plans: We currently require that operating units identify strategies to address IT Security in their annual IT Strategic Plan, and an update of their compliance with the Department IT Security Program requirements in their annual Operational IT Plan. We are not clear how we fail to meet this requirement. Also, if more detail is required, we are uncertain how this can be accomplished without revealing security weaknesses in a public document. We would appreciate further guidance concerning the approach and level of detail expected in such a reporting.
10. Issue-specific IT security policy on Internet usage, e-mail, web security, and communications.	We agree and will ensure that these issues are included in the self assessment. See II.1 below.
II CIO Has Taken Steps to Improve IT Security, But Additional Efforts Are Needed	
In addition to the oversight of operating unit self-assessments using the CIO Council Framework, we recommend that the CIO commit to an operating unit compliance review program that extends beyond the FY 2001 and 2002 requirement of the recent Government Information Security Reform Act. Reviews should begin as soon as possible and should ensure that operating units:	We agree that the requirements of the Government Information Security Reform Act need to be continued into future years. We agree that better compliance review is necessary. Unfortunately, even with the addition of one IT Security staff member, hands-on compliance review of operating unit systems by the OCIO in FY

Additional Focus Needed on Information Technology Security Policy and Oversight **Draft Inspection Report No. OSE-13573/February 2001** **Draft Comments on Recommendations** March 29, 2001	
OIG Recommendation	OCIO Comment
	2001 will not be possible in time to fulfill the OMB requirements of this Fall. Therefore, for this year, we plan to use the Federal CIO Council's Security Assessment Framework in a self-assessment model. We will then measure the success of this approach and plan for future years accordingly. It is our goal, in future years, to add hands-on compliance reviews as resources permit.
1. Have program-level, issue-specific, and system-level policy in place that complies with federal IT security policy and the Department's revised program-level policy.	We agree. The draft questionnaire prepared by NIST in support of the Framework addresses this issue.
2. Implement formal IT security awareness and training programs.	We agree. The draft questionnaire prepared by NIST in support of the Framework addresses this issue.
3. Develop incident response capabilities.	We agree. The draft questionnaire prepared by NIST in support of the Framework addresses this issue.
4. Report deficiencies in IT security as material weaknesses pursuant to OMB Circular A-123 and FMFIA.	See I.9 above.
5. Include IT-related procurement specifications for hardware, software or services, to ensure that they include adequate security requirements and/or specifications that are commensurate with the sensitivity of the system, and that security requirements are included in operating unit budgets. The CIO should work with the Department's Office of Acquisition Management and the Office of Budget to ensure	We agree and will ensure that these issues are included in the self assessment. We agree. This is already being done for major systems that require an Exhibit 300B submission to OMB. We will begin liaison with the Office of Acquisition Management and the Office of Budget to ensure implementation for other systems.

Additional Focus Needed on Information Technology Security Policy and Oversight **Draft Inspection Report No. OSE-13573/February 2001** **Draft Comments on Recommendations** March 29, 2001	
OIG Recommendation	OCIO Comment
implementation.	
6. We also recommend that the review program include procedures to review on a sample basis operating unit IT security documents to determine that:	We agree that quality of assessments and plans should be emphasized in addition to quantity.
a. IT security plans are prepared for all sensitive systems and that they comply with NIST SP 800-18.	We agree and will begin a program to review IT Security plans on a sample basis as resources permit.
b. Systems are accredited and that a management official was involved in the accreditation process.	We agree. We have recognized through your review, and that of the GAO, that our accreditation process needs improvement. We plan to require that the CIO be the liaison between the certification and accreditation processes in order to introduce a technical to business translator.
c. Verification reviews of individual systems are conducted at least every three years or when significant modifications are made to systems and that the scope of the reviews is appropriate based on system risk.	We agree and will ensure that these issues are included in the self assessment.
d. Systems are audited periodically for illegal software or that some other mechanism exists for ensuring that only legal copies of software are being used.	We agree and will ensure that these issues are included in the self assessment.