U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Additional Improvements Needed To Strengthen NIST's Information Security Program

Final Inspection Report No. OSE-15078/September 2002

PUBLIC RELEASE

Office of Systems Evaluation

CONTENTS

EXECUTIVE SUMMARY

Information technology is critical to NIST's mission. Much of NIST's research and other work depends on computer models, computer data, and other electronic information. With this increasing reliance on computing technologies, including the use of the Internet and its related information dissemination techniques, the potential for loss, compromise, and misuse of NIST data and systems grows daily.

The objective of our evaluation was to determine whether NIST's information security program for unclassified systems complies with the Government Information Security Reform Act (GISRA), which mandates that federal agencies have effective security for the information resources supporting their operations and assets. Using NIST's *Security Self-Assessment Guide for Information Technology Systems*, as recommended by OMB, we evaluated NIST's information security policies and procedures, roles and responsibilities, and adherence to applicable laws, regulations, and guidance.

We found that NIST is taking steps to improve information security such as increasing its computer security staff, developing issue specific security policies, and implementing a formal computer security incident reporting and handling process. Yet many important security requirements have not been met. Our evaluation found the following issues:

- NIST lacks a comprehensive information security program policy. Its current policy does not address critical roles and responsibilities and management control elements, such as risk management, review of security controls, and certification and accreditation[1] that are required by GISRA. (See page 8.)

- NIST's policy assigns responsibility for authorizing system operations (also called accreditation) to the CIO, but not to the senior official whose mission the system supports. The CIO and the appropriate senior official should be co-accrediting officials. (See page 9.)

- None of NIST's 109 identified operational systems has a documented risk assessment or an approved security plan. Moreover all but two lack accreditation. (See pages 10 and 11.)

- NIST has established a schedule to complete its risk assessments, security plans, and accreditations. We are concerned however, that the schedule may be too ambitious to permit sufficient analysis, documentation, and review. (See page 12.)

- NIST's Sensitive Information Technology System Inventory did not include at least three operational systems from one laboratory, suggesting that there may be

[1] Certification is the formal testing of the security safeguards implemented in a computer system to determine whether they meet applicable requirements and specifications. Accreditation is the formal authorization by management for system operation, including an explicit acceptance of risk.

additional systems at NIST that have not been identified and should be included in that inventory. (See page 14.)

- NIST does not ensure that external researchers and collaborators who have no further need for system user accounts are removed from NIST computer systems in a timely manner, thus leaving its systems vulnerable to unauthorized access. (See page 15.)

- Risk designations assigned to some positions are inconsistent with their levels of responsibility and trust. Employees filling these positions have not received the appropriate level of background investigation, thus increasing the potential for an individual in a position of public trust to potentially cause harm to the efficiency and integrity of NIST programs and operations. (See page 16.)

- NIST does not have a process in place for effectively planning and controlling information technology investments across the organization and therefore lacks a means of ensuring that information security requirements and costs are appropriately addressed in capital asset planning. (See page 17.)

- NIST does not have a CIO; its CIO office resides in the Information Technology Laboratory (ITL) and reports to ITL's acting director, who also serves as the acting CIO. We believe that an empowered CIO—that is, one that has the support of the NIST director and sufficient resources—is essential for improving NIST's information security program, as well as its management of its IT resources in general. (See page 20.)

Since the completion of our fieldwork, the director of NIST has taken important steps toward improving information security by issuing a memorandum acknowledging his responsibility for the security of NIST's data and IT systems and directing all members of NIST's upper management to give information security high priority and ensure that the agency's policies, procedures, and operational environment are exemplary. (See page 20.)

We made numerous recommendations for improving information security (see pages 10, 14, 16, 17, 19, and 21).

…

NIST's response to our draft report stated that it generally agreed with our findings and recommendations and described actions being taken or planned. Following each set of recommendations, we have included a brief synopsis of NIST's response and, where appropriate, our comments.

Although the response indicates that the schedule for accreditation has been extended, we remain concerned that it still does not allow enough time to adequately complete all needed analysis, documentation, and testing. We discuss NIST's response and our concerns regarding this matter on page 14. NIST's response to our draft report is included in its entirety as the attachment.

INTRODUCTION

Automated teller machines, atomic clocks, mammograms, and semiconductors are among the innumerable products and services that rely in some way on the work of the National Institute of Standards and Technology (NIST). NIST's mission is to develop and promote measurements, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. Most of NIST's work is done at two locations–Gaithersburg, Maryland, and Boulder, Colorado. The agency has a staff of more than 3,000 full time scientists, engineers, technicians, and support personnel, plus 1,600 visiting researchers and 2,000 collaborators at affiliated centers around the country and overseas.

An ever-increasing amount of NIST's work depends on computer models, computer data, and other electronic information. With NIST's increasing reliance on computing technologies, including the use of the Internet and its related information dissemination techniques, the potential for loss, compromise, and misuse of NIST data and facilities has grown tremendously.

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

Under GISRA, information security is the responsibility of federal agency senior management—the agency head, senior line managers, and the chief information officer (CIO). Other senior officials are responsible for assessing security risks associated with operations and assets for the programs and systems they control. Each agency head is charged with ensuring the security of information and information systems through promotion of security as an integral component of that agency's business operations. Each head is also charged with ensuring that an information security plan to safeguard the privacy, confidentiality, and security of federal information is carried out throughout the life cycle of each system. In turn, the Secretary of Commerce has charged all departmental operating unit heads with these same responsibilities for their organizations, directing them to give information security high priority, sufficient resources, and their personal attention.[1]

The department CIO is required to administer the information security program agency wide. This entails developing the security program, ensuring that the program is effectively implemented and maintained, training and overseeing personnel with significant responsibilities for information security, and assisting other senior agency officials with their information security responsibilities.

GISRA also requires all federal agencies to perform annual reviews of their security programs and the Office of Inspector General (OIG) for each agency to conduct

[1] Memorandum from Donald Evans to Secretarial Officers and Heads of Operating Units, "High Priority to Information Technology (IT) Security," July 27, 2001.

independent evaluations of agency information security programs. As part of our work under GISRA, this report presents our evaluation of NIST's agencywide information security policies and procedures.

Our 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

Founded in 1901, NIST is a non-regulatory federal agency within the Department of Commerce. The agency carries out its mission through four cooperative programs:

- **NIST Measurement and Standards Laboratories** – Eight laboratories employing physical and engineering scientists who provide leadership for vital components of the technology infrastructure needed by U.S. industry to continually improve its products and services.

- **Advanced Technology Program** – A competitive program that provides cost sharing awards to industry for development of high-risk technologies with broad economic potential, such as computer hardware, computer systems, and software applications.

- **Manufacturing Extension Partnership** – A nationwide network of local centers offering technical and business assistance to smaller manufacturers.

- **Malcolm Baldrige National Quality Award** – A highly visible, quality outreach program that recognizes business performance excellence and achievement by U.S. manufacturers, service companies, educational organizations, and health care providers.

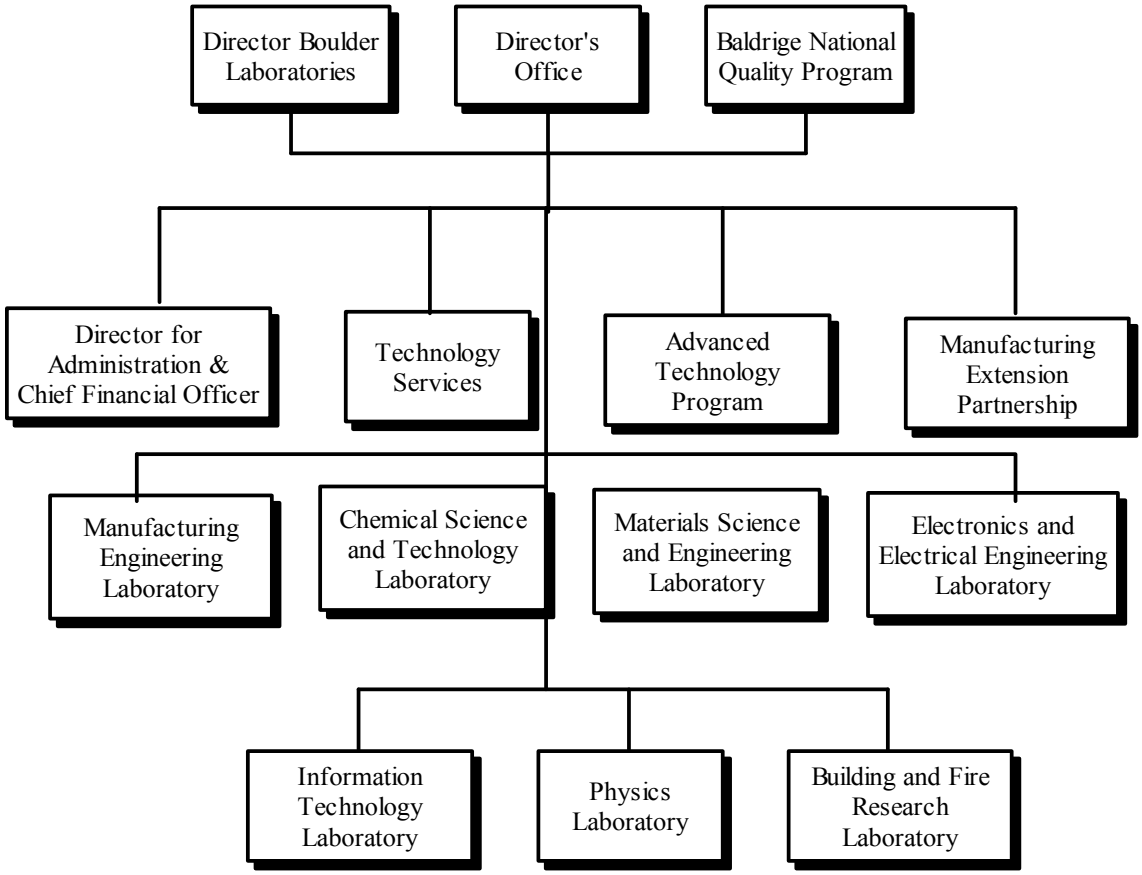
NIST's Allocation of Information Security Responsibilities

Responsibility for information security is distributed among NIST's operating units (Figure 1). Key roles and responsibilities are described here and in Appendix A.

According to Chapter 11 of NIST's Administrative Manual, the director of the Information Technology Laboratory (ITL), with the approval of the NIST deputy director, appoints the NIST computer security officer. The computer security officer develops and implements the computer security program.

Unit directors are required to appoint a security officer to implement the security program within their units. According to NIST, these responsibilities are generally considered collateral duties.

Figure 1. NIST Organization Chart



OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of our evaluation was to determine whether NIST's information security program for unclassified systems complies with GISRA, which seeks to achieve effective security for information resources supporting federal operations and assets. Our evaluation covered NIST's information security policies and procedures as well as their attendant roles and responsibilities, and adherence to applicable laws, regulations, and guidance.

To satisfy the objective, we reviewed NIST's information security policies and procedures, NIST's self-assessments of information systems and security controls that comprised its fiscal year 2001 GISRA submission, and its Corrective Plan of Action and Milestones.

In addition, we interviewed the acting CIO and directors, deputy directors, and information security officers of the Advanced Technology Program and of the Manufacturing Engineering, Information Technology, and Physics laboratories. We also interviewed the director of Human Resources, the NIST computer security officer, and members of NIST's budget staff.

We used as criteria OMB Circular A-130,[2] Appendix III, Security of Federal Automated Information Resources; NIST's Security Self-Assessment Guide[3] (control areas listed in Table 1); the Computer Security Act of 1987; and GISRA.

Table 1. NIST Security Control Areas

Management Controls	Operational Controls	Technical Controls
• Risk Management • Review of Security Controls • Life Cycle • Certification and Accreditation • System Security Plan	• Personnel Security • Physical Security • Production, Input/Output Controls • Contingency Planning • Hardware and System Software Maintenance • Data Integrity • Documentation • Security Awareness, Training, and Education • Incident Response Capability	• Identification and Authentication • Logical Access Controls • Audit Trails

[2] Office of Management and Budget. 1996. Circular No. A-130: Management of Federal Information Resources. Washington, D.C.: Office of Management and Budget Executive Office.

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

Our fieldwork was conducted from March through May 2002. We held an exit conference on July 19, 2002, with the NIST deputy director, acting CIO, computer security officer, and members of their staff. NIST officials generally agreed with our findings and recommendations.

FINDINGS AND RECOMMENDATIONS

I. NIST Is Taking Steps To Improve Its Information Security Program

OMB Circular A-130 and GISRA require that federal agencies develop, implement, and administer agency wide information security programs that include policies, procedures, and controls that afford security protections commensurate with the risk and magnitude of harm. GISRA further requires that agencies:

- ensure that information security plans are in effect throughout the life cycle of the system,
- establish appropriate levels of security,
- periodically test and evaluate security controls,
- designate a security official who reports to the CIO,
- train personnel with information security responsibilities,
- provide security awareness training, and
- establish procedures for detecting and responding to computer incidents.

Our evaluation found that NIST has taken several steps to make its information security program more effective and bring it into compliance with current departmental and federal IT security policies. For example:

- In FY01, NIST increased its computer security staff from one full-time staff member to four to better assist operating units with improving their security posture and compliance with policies, develop formal security awareness and training programs, and address security issues resulting from the rapid expansion in NIST's use of information technology.

- NIST also developed and published issue-specific information security policies, procedures, and guidance that address current and relevant concerns, such as, the computer intrusion response team operating policy, incident reporting procedures, the undesirable e-mail policy, the firewall policy, the information technology resources access policy, and communications, security planning, and telecommuting policies.

- The NIST information security officer developed and posted to the security web site a system security plan template, guidance, and a list of frequently asked questions to assist unit computer security officers in developing their system security plans. Also posted to the security web site were templates for the NIST SP 800-26 self-assessment questionnaire and a contingency plan based on NIST SP 800-34.

- NIST hired a contractor to support, throughout FY02, completion of risk assessment activities that involves development of a comprehensive risk assessment methodology, a broad-based risk assessment, a focused risk

assessment for four identified critical systems, and preparation of the FY02 GISRA report.

- NIST developed and implemented a formal information security awareness and training program. All new employees, as part of their orientation, are briefed by the IT Security Office on the NIST Information Security Program, proper use of NIST's information resources, and procedures for reporting computer incidents. (In April 2002, NIST held its first "Annual Computer Security Day" at the Gaithersburg and Boulder campuses, in an effort to initiate periodic refresher training. The one-day event included guest speakers, updates on various computer security efforts, information on NIST Computer Security Division services, and information on vendor products.)

- NIST also established and implemented a formal and documented information security incident reporting and handling process consistent with OMB Circular A-130 and GISRA requirements. As part of this effort, NIST fielded an intrusion detection system (IDS). Data from the IDS and firewalls are transmitted to the incident response team for review and analysis and electronically transmitted to the General Services Administration's Federal Computer Incident Response Center (FedCIRC) for analysis.

II. Information Security Policy and Procedures Are Missing Key Control Elements

While NIST is taking steps to improve its information security program, its security program policy is missing critical elements, and certification and accreditation procedures need to be strengthened.

A. NIST Lacks A Comprehensive Security Program Policy

An effective information security program requires clear direction from senior management. Senior management must assign security responsibilities to organizational elements and individuals and must formulate the security policies that become the foundation for the organization's security program. These policies must be based on an understanding of the organization's mission priorities and the assets and business operations necessary to fulfill them. They are also the primary mechanism by which management communicates its views and requirements and establishes cost-effective organizational and system security controls.

Chapter 11 of NIST's Administrative Manual establishes the foundation for NIST's security program and its use by the operating units. It specifies policies regarding the security of computing resources and assigns roles and responsibilities for information security to organizational elements.

We found, however, that the manual is missing critical information security control elements required by GISRA. Specifically, the policy does not assign responsibilities to the director of NIST and to the CIO for developing, implementing, and maintaining an

agencywide security program. The policy also lacks key controls, including risk management, review of security controls, life cycle management, certification and accreditation, and contingency planning. As discussed in this report, improvements are needed to better implement these controls.

Establishment of a comprehensive information program that includes a security management structure and a documented up-to-date security plan or policy is required for the protection of sensitive data and resources. Protecting mission critical data is essential to the success of NIST's information security program.

On its computer security web site, NIST has posted a document titled "Recommended NIST Computer Security Procedures," but it contains policies, not procedures. We were told the document was so titled because of the difficulty getting a policy document approved; it was reportedly easier to circulate this document under the guise of "procedures." Consequently, there is confusion because required baseline security policies are stated as "recommended" procedures, which by definition, do not have the same impact as required policy. Incorporating the appropriate sections of this document into NIST's security program policy would reduce confusion and provide users with a single, comprehensive policy statement.

B. Draft Certification and Accreditation Procedures Should Be Strengthened

OMB Circular A-130 requires senior management officials whose mission could be adversely affected by security weaknesses to formally authorize the use of a system before it becomes operational. This authorization, also referred to as accreditation, denotes that the manager understands and accepts responsibility for risks associated with putting the system into operation. Authorization is based on a certification, the formal assessment of the management, operational, and technical controls. The security plan documents the system's protection requirements and security controls currently in effect. The certification along with the security plan forms the basis for management's decision to authorize processing. A system should be reauthorized following any significant change or every three years at minimum, more often where risk and potential magnitude of harm are high.

NIST's policy assigns the role of authorizing official to the CIO but not to the manager whose mission the system supports. The rationale is that the CIO is responsible for NIST's technology infrastructure, and because most systems are tied to that infrastructure, vulnerabilities in one system would leave the entire network vulnerable. For those interconnected systems, NIST should designate the senior management official and the CIO co-accrediting officials since the mission of both managers could be adversely affected by information system security weaknesses. For standalone systems, the senior mission manager can be the single accrediting official.

Recommendations

We recommend that the director of NIST ensure that NIST managers take the following actions to achieve compliance with GISRA and other applicable laws, regulations and guidance:

1. Update and expand Chapter 11 of the Administrative Manual to provide a comprehensive information security program policy:

    a. Ensure that all roles and responsibilities for information security, including those of the director and CIO, are explicitly identified and documented and consistent with GISRA requirements.

    b. Review the security document, "Recommended Computer Security Procedures," for incorporation of appropriate sections into Chapter 11 as policy, and supplement it with additional policy and procedures as needed.

2. Revise policy on accreditation to designate as accrediting or co-accrediting officials those senior officials whose mission could be adversely affected by information system security weaknesses.

Synopsis of NIST's Response

The response stated that a revision to Chapter 11.02 of the NIST Administration Manual, which expands the information security policy, has been drafted and is being reviewed by management. A modification to the certification and accreditation policy has also been drafted making operating unit directors and the NIST CIO co-accrediting officials. The response noted that this policy change will not be implemented until FY03; in FY02, systems will be accredited only by the operating unit directors.

III. Management Controls Are Not Fully Implemented and Schedules Are Unrealistic For Achieving Adequate Product Content and Quality

Senior management officials are responsible for controlling risks within their information systems. Management controls include risk management, review of security controls, life cycle management, certification and accreditation, and system security plans. At NIST, risk assessments have not been completed, security plans have not been finalized, and the majority of its systems are operating under interim authority (that is, they have not been accredited). Schedules for completing these tasks are too aggressive to provide the intended degree of assurance.

A. Risk Assessments Have Not Been Completed

GISRA requires program officials to determine and assess risks to the operations and assets they control. OMB Circular A-130 no longer requires agencies to prepare formal risk analyses but does require them to use a risk-based approach to determine adequate

security. This means security must be commensurate with the risk and magnitude of potential harm resulting from the loss, misuse, or unauthorized access to or modification of information. Risk assessments should incorporate (1) the value of the system or application, (2) the possible costs of enacted threats or exploited vulnerabilities, and (3) the effectiveness of current or proposed safeguards. Assessing risk to a system is an ongoing necessity, ensuring that new threats and vulnerabilities are identified so appropriate security measures can be implemented.

Although we found that none of NIST's 109 identified operational systems have documented risk assessments, in March 2002 during our evaluation, NIST awarded a contract to develop a comprehensive risk assessment methodology and conduct a broad-based risk assessment and a focused risk assessment for four critical systems. Once developed, the risk assessment methodology will be used by unit security officers to complete their individual risk assessments. NIST expected the methodology to be completed on June 30, 2002, and required the remaining risk assessments be completed by July 26, 2002. As of July 2, 2002, the methodology was received and distributed to several operating units for feedback. However, at the time of our exit conference on July 19, the assessment methodology had not been distributed to all operating units for use.

B. Systems Are Operational with Only Draft Security Plans in Effect

Security plans provide an overview of the system's security requirements and describe the methods used to assess the nature and level of risk to the system. These plans are based on an analysis of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. At NIST, the unit security officer, who represents the business area that will use the system, works with the system owner to prepare and maintain the plan. The Computer Security Act of 1987 requires that security plans be reviewed annually and revised as needed to ensure that security controls can handle significant changes to the system as well as rapidly changing threats.

All of NIST's inventoried systems have draft security plans. Between March and April 2002, the NIST security officer informed all system owners of the schedule requiring final security plans for all systems to be completed by July 26, 2002.

C. Systems Are Not Accredited

OMB Circular A-130 requires management officials to formally authorize, based on an assessment of the management, operational, and technical controls, the use of a system before it becomes operational. This accreditation denotes that the manager understands and accepts responsibility for risks associated with putting the system into operation. The security plan establishes and documents system protection requirements and security controls in place, and thus forms the basis for management's decision to authorize processing.

We found that with the exception of two systems, all of NIST's operational systems are operating without accreditation. Although these systems have been granted interim authority to operate, the lack of accreditation indicates that management has neither formally reviewed the controls nor explicitly accepted the associated risk, and therefore there is no assurance that NIST's operational systems are adequately protected. NIST is requiring that all documentation needed to support accreditation be submitted to the information security officer by August 15, 2002.

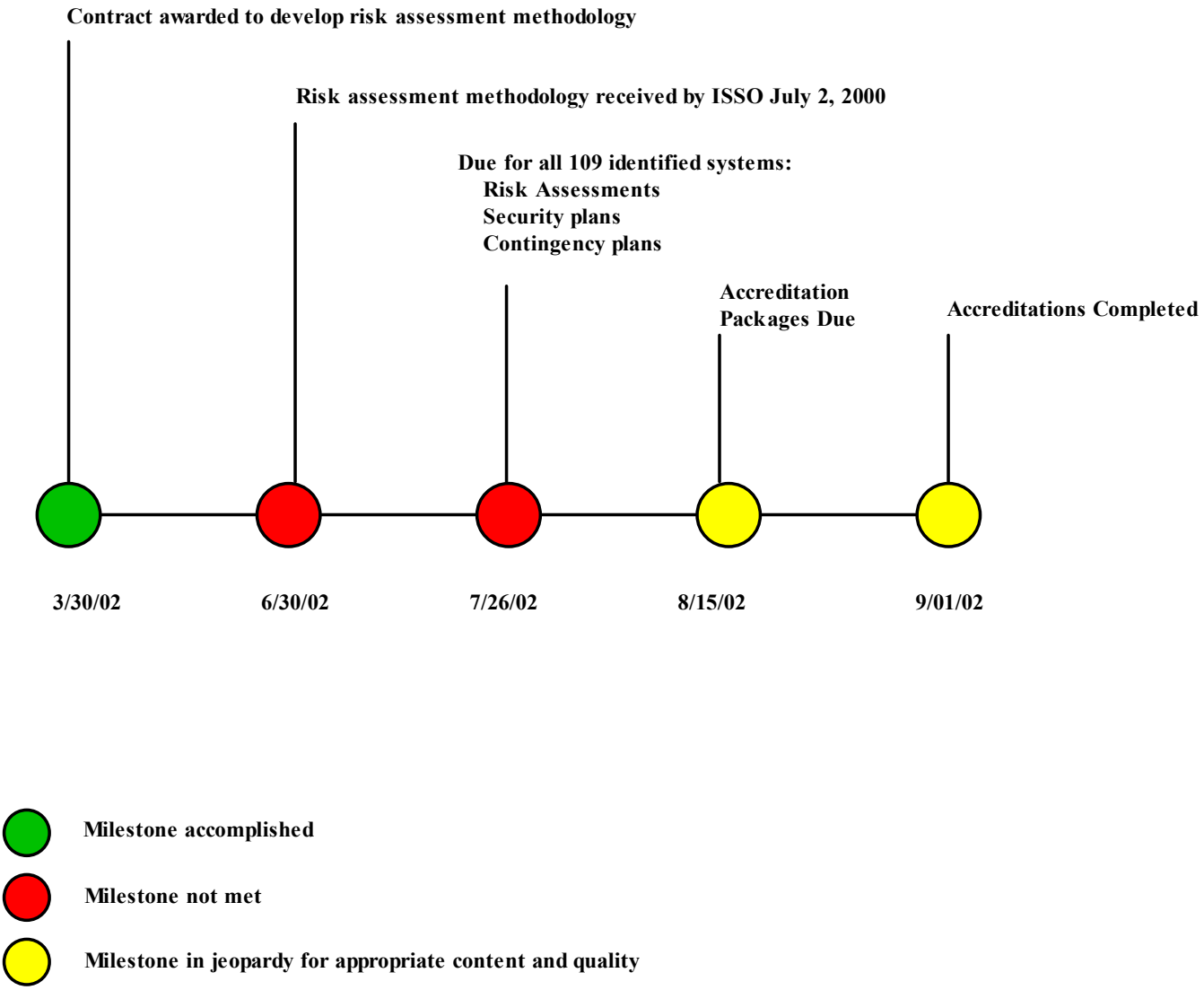
D. Deadlines for Security Plans and Accreditations Are Unrealistic

Requirements for security plans and accreditations are not new. For example, the Computer Security Act, passed in January 1988, mandated federal agencies to establish, within one year, a plan for the security of each of its computer systems and to revise the plan annually if necessary. However, many federal agencies, including NIST, have not fully implemented these requirements. As a result of GISRA and oversight by OMB and the Department, they are now under intense pressure to do so. Therefore, the Department has established a deadline for completion and approval of all security plans by the end of September 2002. In response, NIST is requiring all final security plans by July 26; it also has established a deadline for accreditation packages by August 15 and completion of accreditation by August 30.

To meet these deadlines, NIST posted guidance to units on its web site that established milestones for final system security plans, completed certifications, and submission of accreditation packages for its 109 identified operational systems as described in Figure 2. We believe that these milestones do not allow enough time for quality processes and products. Furthermore, although NIST received a risk assessment methodology from its contractor on July 2, at the time of our exit conference (July 19), the methodology had still not been distributed to all units so that they could conduct their risk assessments. As all the future dates depend on the risk assessments having been done by July 26, this delay has ramifications for all subsequent dates. Given this schedule slippage, we are concerned that the current schedule will not allow sufficient time for the remaining work in this area.

We concur that these important activities need to be completed as soon as possible, but are concerned about the quality of the plans and certifications that will result from this aggressive schedule. Given the delay, the proposed schedule appears to place an unreasonable burden on the information security staff, which needs sufficient time to ensure the appropriate product content and quality for the security plan and accreditation package submissions before they are approved. NIST needs to ensure that its security plans and certifications and accreditation are of sufficient quality to impart the intended degree of assurance.

Figure 2. Timeline for Information Security Activities



E. System Inventory May Not Reflect Actual Number of Operational Systems

During our evaluation we identified three Advanced Technology Program operational systems (electronic submission system, electronic proposal review, and proposal management system) that were not included in NIST's Sensitive Information Technology System inventory. The inventory is used to identify and track status of information of all systems subject to security controls (risk assessments, security plans, and accreditation). Our concern is that there may be additional systems at NIST that have not been identified and need to be added to the inventory. If systems are omitted from the inventory, they may not receive the attention needed to ensure that their security is effectively managed. Guidance on determining how to identify systems subject to security controls is contained in the security planning's "frequently asked questions" section on NIST's intranet and is limited to a definition from NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*.[4] NIST should expand on the key aspects of the guidance contained in NIST SP 800-18 and ensure that it is readily available to the units and applied appropriately.

Recommendations

We recommend that the director of NIST ensure that NIST managers take the following actions:

1. Develop a schedule that allows sufficient time for completing and approving risk assessments, security plans, and accreditations to enable staff to provide adequate product content and results that impart the intended degree of assurance.

2. Accredit all operational systems and update accreditations for all operational systems every three years, at a minimum, or whenever a significant change in the system occurs.

3. Extract key aspects of the guidance contained in NIST SP 800-18 on how to identify systems subject to security controls and ensure that it is readily available to the units and applied appropriately.

4. Review system inventory to ensure that all systems, particularly those subject to security controls, are included.

Synopsis of NIST's Response

The response indicated that the risk assessment methodology was delivered to NIST's operating units on July 22, and the deadline for completing system accreditation was extended to September 30. It further stated that in FY03, NIST's IT security officer will

[4] National Institutes of Standards and Technology. 1998. *Guide for Developing Security Plans for Information Technology Systems*. Gaithersburg, MD: National Institutes of Standards and Technology.

conduct an independent review of certified and accredited systems and make recommendations to the NIST CIO.

NIST's response also noted that system owners were provided with additional guidance on system boundaries and directed to reassess the system inventory. The reassessment resulted in an inventory of 109 operational systems.

OIG Comments

Given the complexity and importance of the activities required to accomplish certification and accreditation, including testing the security controls to ensure that they perform as intended, we remain concerned that even with the schedule extension, there is not enough time to adequately complete all of the requisite activities and documentation. We believe that the accreditations should be considered provisional until there is confirmation that each system has all needed security controls and that these controls have been tested to ensure they perform as intended.

The previous inventory had 130 operational systems. The revised number (109) is reflected throughout our final report.

IV. Security Controls Are Not Extended to External Collaborators and Researchers

During our review, we found problems with NIST's management of user accounts for external collaborators (researchers who do not reside at NIST's Gaithersburg or Boulder campus) left NIST's systems vulnerable to unauthorized access. Under the current process, system administrators and unit information security officers who are responsible for maintaining access to NIST resources are not always informed when external collaborators no longer need access to NIST resources. Often they find out months or even years later that a person no longer requires access and that the account should have been closed. This situation was documented in Manufacturing Engineering Laboratory's system security plan as an operational controls weakness. A similar issue was noted in the Department's Consolidated Financial Statements FY 2001,[5] where it was reported that NIST needed to implement procedures to ensure that departing employees' system user accounts are removed from computer systems in a timely manner

NIST is currently addressing this issue for its own employees and researchers, working on each campus. NIST is also developing systems to track employees and resident guest researchers; however, these systems do not address collaborators and researchers who are not on NIST campuses but who use NIST computing resources.

[5] U.S. Department of Commerce. 2002. *Improvements Needed in the General Controls Associated with the Department's Financial Management Systems*, Consolidated Financial Statements FY 2001. Washington, D.C.: U.S. Department of Commerce.

Recommendation

We recommend that the director of NIST ensure that NIST managers verify that systems administrators and information security officers are promptly notified when external researchers and collaborators no longer need access to NIST resources.

Synopsis of NIST's Response

The response noted that in FY01, NIST began developing a system for tracking guest researchers who have a NIST badge and that the system will be expanded to include tracking of all guest researchers and external collaborators.

V. Risk Levels for Positions Have Not Been Properly Assigned

NIST has numerous positions that involve policymaking, major program responsibility, and other duties demanding a significant degree of public trust. These types of positions are normally designated as high- or moderate-risk positions. Agency heads are required to designate every competitive service position within the agency at a high-, moderate-, or low-risk level as determined by the position's potential for adversely affecting the efficiency and integrity of government programs and operations.[6] These designations are important because they determine the depth of background investigation required.

We reviewed risk level designations for positions held by employees of the Advanced Technology Program and the Mechanical Engineering, Information Technology, and Physics laboratories. With the exception of ITL, all had positions with risk designations that were inconsistent with their levels of responsibility and trust. For example, system administrators and information security officers—whose work responsibilities directly affect government programs and operations—were designated as low risk; thus employees filling these positions had not received the level of background investigation commensurate with the risk level of their responsibilities. The ITL managers, however, had already reviewed employees' position designations, assigned appropriate risk levels, and submitted paperwork to conduct the appropriate background investigation required by their new proposed designation.

In a previous effort to identify the criteria used Department-wide to determine appropriate risk levels and their associated background investigations, we noted a lack of guidance from the Department's Office of Human Resources Management (OHRM) and the Office of Security (OSY). We addressed this issue in our report, *Program for Designating Positions According to Their Risk and Sensitivity Needs to Be Updated and Strengthened*, Final Inspection Report No. OSE-14486/September 2001, which includes recommendations that the Department provide to operating units, updated guidance for determining appropriate risk levels and their associated background investigations. Both OSY and OHRM agreed to provide updated guidance based on OPM regulation and guidance and ensure that roles and responsibilities of heads of operating units,

[6]Positions designated as low risk are not considered "public trust" positions.

subordinate managers and supervisors, servicing personnel officers, and security officers are clearly stated. Thus, NIST needs to ensure that its efforts to review and appropriately adjust the risk levels associated with sensitive positions are consistent with the Department's forthcoming guidance.

Recommendation

We recommend that the director of NIST take the necessary actions to ensure that NIST managers work with the Department's Office of Human Resources and Office of Security to verify that all current positions are properly designated according to risk and that appropriate background investigations are conducted for all NIST staff.

Synopsis of NIST's Response

The response stated that the director will issue a memorandum to NIST operating units directing that all personnel who hold system administrator privileges to access any NIST server must have an ADP risk level of either moderate or high.

OIG Comments

This action will only partially address our recommendation. In addition to system administrator positions, NIST has numerous positions that involve policymaking, major program responsibility, and other duties that demand a significant degree of public trust. These types of positions are normally designated as high- or moderate-risk. All positions should be reviewed to determine whether they are properly designated according to risk.

VI. NIST Has Not Implemented a Capital Asset Planning Process

The 1996 Clinger-Cohen Act attempted to address longstanding problems and eliminate failures in the federal government's acquisition and use of IT by calling for agencies to establish a capital planning and investment control process—applicable to all IT capital assets[7]—to help ensure that appropriate IT projects are funded and well managed and that planning, budgeting, acquisition, and management of IT resources are integrated. In response, Commerce established an IT capital planning and investment control process at the Department level for projects requiring special attention[8] and required each operating unit to implement a process of its own.

[7] OMB Circular A-11 defines an IT capital asset as IT that is used by the federal government and has an estimated useful life of two years or more. Capital assets do not include items acquired for resale in the ordinary course of operations or items that are acquired for physical consumption, such as operating materials and supplies.

[8] Projects that merit special attention are (1) Department-wide or interagency systems; (2) those with political sensitivity, mission criticality, or risk potential; (3) those with life cycle costs higher that $25 million; or (4) those experiencing difficulties.

GISRA and OMB policy note that information security must be a component of the system's architecture and implemented and managed throughout the system's life cycle. Thus agencies are required to identify and budget for security measures and resources needed to protect their IT investments throughout the investment's life cycle. OMB Circular A-11,[9] stipulates that each agency's annual budget request, in Exhibit 53, "Agency IT Investment Portfolio," must include security costs for its IT projects as a percentage of the total system cost or project investment. Also, a capital asset plan (Exhibit 300) must be provided for each major IT project;[10] it must indicate whether the project's information security meets GISRA requirements and describe the security and privacy measures to be used.

Despite these objectives and requirements, NIST does not have an IT capital planning and investment control process. As a consequence, it lacks a mechanism to ensure that information security is properly planned and budgeted. Its life cycle management manual for IT, which addresses capital investment planning, is in draft and has not been implemented; and its IT Policy Council, which is to perform oversight of the process, has not begun to do so.[11] An official in the NIST CIO's office told us that this process will be prototyped in ITL prior to NIST-wide implementation, but no date has been scheduled for finalizing and implementing the process.

In its budget guidance for FY 2003, the NIST budget office advised that because of increased scrutiny of IT expenditures, particularly those related to information security, additional detail would be required to support budget requests. Specifically, each unit was required to designate how much of its total IT spending was for information security, with costs presented in five categories: program planning and management; evaluation and testing; technical controls; security awareness, training, and education; and incident response. Each unit's information was consolidated into a NIST-wide Exhibit 53. However, the NIST CIO's office provided neither guidance nor review of these costs, leaving their validity questionable. A capital asset planning process would assist NIST in integrating the IT and budget processes.

In guidance for IT budgeting for FY 2004, the Department CIO identified NIST's Grants Management Information System as a major system requiring a capital asset plan, reflecting OMB's increased attention to grants management. The guidance also stated that all new IT investments, as well as modifications and enhancements of existing systems which exceed base funding, must be described in capital asset plans at a level of

---

[9] Office of Management and Budget. 2001. Circular A-11 Washington, D.C.: Executive Branch Office of Management and Budget.

[10] A major IT project requires special management attention because of its (1) importance to an agency's mission; (2) high development, operating, or maintenance costs; (3) high risk; (4) high return; or (5) significant role in the administration of an agency's programs, finances, property, or other resources. Major IT projects must have the concurrence of the chief information officer.

[11] NIST's IT Policy Council consists of operating directors, the CIO, a technology services senior representative, Director for Administration/Chief Financial Officer senior representative, operating unit deputy directors, and a Management Advisory Council representative.

detail commensurate with the size of the investment. The guidance also stated that IT initiatives must be a product of the operating unit's capital planning and investment control process.

Without a planning and control process developed to deal with IT investments and information security specifically, NIST cannot ensure that IT projects are appropriately selected, planned, and managed; that information security is a factor in each system's design and a management consideration throughout its life cycle; or that information security cost estimates are valid.

Recommendations

We recommend that the director of NIST take the necessary action to ensure that a deadline is established for finalizing and implementing an IT capital planning and investment control process that includes information security with the budget process.

Synopsis of NIST's Response

The response stated that a capital investment planning process was begun in FY02 and will be fully implemented in FY03.

VII. Proactive Attention from NIST Senior Management Could Improve Information Security

To safeguard the privacy, confidentiality, and security of federal information, GISRA requires the head of each agency to ensure that the agency's information security plans are carried out throughout the life cycle of each of the agency's systems. The agency head is also responsible for promoting security as an integral component of that agency's business operations; and agency managers and program officials are required to ensure that effective security policies and procedures are implemented throughout the life cycle of every IT system.

As the discussion in the preceding section indicates, until recently, information security at NIST has not received adequate attention, and significant weaknesses exist in planning, budgeting, implementation, review, and oversight. Thus there has been a lack of follow through in carrying out fundamental responsibilities, including:

- establishing comprehensive information security policies and procedures;
- identifying, assessing, and understanding risks to NIST's IT assets;
- determining information security needs commensurate with the levels of risk;
- planning, implementing, and testing controls that adequately address risk;
- continually monitoring and evaluating policy and effectiveness of information security practices;

- ensuring appropriate personnel security controls are implemented; and

- developing a capital planning and investment control process and integrating information security into it.

In June 2001, to reinforce the Department's management of IT and its capital investment planning, the Secretary issued a memorandum directing all operating units to appoint a CIO who would report to the head of the operating unit or the principal deputy, as well as to the Department's CIO.[12] The objective: to have a senior official in each operating unit with the stature, skills, and clout to strengthen IT management. The CIO is to be responsible for advising the operating unit's senior management on all aspects of IT and is to concur in the budgeting and expenditure of funds for IT by the unit. To further highlight the importance of information security as a senior management responsibility, the Secretary of Commerce, in a July 2001 memorandum, directed secretarial officers and heads of operating units to give information security high priority and sufficient resources and to invest the time necessary to assure information security improvements. The memorandum further directed these officials to work closely with and support their operating unit CIOs with respect to information security and to allocate sufficient resources at the operating unit level necessary for the protection of Commerce data and systems.

Currently, however, NIST does not have a CIO; its CIO office resides in ITL and reports to ITL's acting director, who also serves as the acting CIO. We believe that an empowered CIO—that is, one that has the support of the NIST director and sufficient resources—is essential for improving NIST's information security program, as well as its management of its IT resources in general. As GISRA makes clear, however, information security is the responsibility not solely of the CIO but of senior management across the organization. Thus, the awareness, support, and proactive involvement of NIST's senior management are vital to establishing the environment and ensuring the resources needed to promote an effective information security program.

Recognizing that its IT management needs improvement, NIST is working to define a new CIO organizational structure intended to enhance its authority and provide a more effective focus on IT oversight, including information security. Since May, when our fieldwork was completed, the director of NIST has taken an important step toward improving IT security at NIST by issuing a memorandum acknowledging his responsibility for the security of NIST's data and IT systems. This memo also directs all members of NIST's upper management to give IT security a high priority and to ensure that NIST policies, procedures, and operational environment are exemplary.[13]

---

[12] Memorandum from Donald Evans to Secretarial Officers and Heads of Operating Units, "Strengthening Commerce Information Technology Management," June 13, 2001.

[13] Memorandum from Arden L. Bement, Jr., to Senior Management Board, "Responsibilities for Information Technology (IT) Security," June 11, 2002.

Recommendations

We recommend that the director of NIST take the following actions:

1. Ensure that information security receives high priority in accordance with the Secretary's direction.

2. Ensure that senior NIST management officials understand and implement their information security responsibilities.

3. Define and implement a new CIO organizational structure, appoint a CIO as soon as possible, and ensure that the CIO is provided with the responsibility and authority to develop and maintain a NIST-wide information security program.

OIG Comment

Although the response did not address how these recommendations will be implemented, the NIST director recently sent a memorandum to the NIST operating unit directors discussing the findings and recommendations of our evaluation and emphasizing his personal responsibility as director and their responsibility as program managers for good information security.[14] Significantly, the memorandum states:

> NIST's highly visible mandate as the provider of cyber-security guidance for Federal Agencies and icon for commercial and industry software providers and users, requires that our own systems meet a "higher standard" of excellence. If we are the premier developer of cyber security guidance, we should also be the premier performer in the implementation of that guidance!

The memorandum further discusses the need to adopt new approaches to information security as part of the NIST "lifestyle." It concludes by pointing our the importance of all employees understanding their responsibilities for information security, the need for NIST management to lead and promulgate changes, and the goal of making NIST an exemplary agency in securing its IT resources.

These are significant steps in addressing the first two recommendations. However, the third recommendation regarding the CIO remains to be addressed. We again emphasize the importance of having an empowered CIO to achieve the needed improvements in information security, in particular, and IT management, in general. We look forward to receiving your approach to implementing this recommendation when you submit your action plan.

[14] Memorandum from Arden L. Bement, Jr., Director, for OU Directors, "NIST IT Security and the Government Information Security Reform Act (GISRA) Audit," September 6, 2002.

APPENDIX A

Additional Information on Security Roles within NIST

Computer Security Officer – Appointed by the Information Technology Laboratory director, with the approval of the NIST Deputy Director, the NIST Computer Security Officer is charged with the following:

- Developing computer security policies and procedures for NIST.
- Coordinating NIST computer policy, computer security actions, and incident reporting with the Department of Commerce and other outside organizations.
- Ensuring periodic training opportunities for NIST staff in the areas of computer security, awareness of problems, and good practices.
- Helping with the planning, budgeting, and implementation of computer security functions for NIST.
- Serving as a resource on effective computer security practices for NIST management and staff.

Operating Unit Directors - Appoint the computer security officer responsible for the security of all information resources in the unit and, for units with multiple sites, appoint a computer security officer for each site. Unit directors are also responsible for assessing risks of loss of unit information resources and implementing appropriate levels of security for their facilities, software, data, and contracted services.

OU Computer Security Officers - Serve as contact points for all computer security related issues for the unit; represent their unit in the development of NIST computer security policy; and recommend to the unit director how best to implement the NIST computer security policy within their unit.

Division Chiefs, Group Leaders, and Project Managers - Ensure that the correct level of computer security is implemented for each resource, given the risks, and that employees have the necessary awareness and computer security training.

System Administrators - Responsible for the computer security program and procedures for systems under their control.

All authorized users (employees and collaborators) - Responsible for complying with policies and procedures on the use of information resources and for reporting to the appropriate unit computer security officer and the NIST computer security officer any suspected breach of security.

ATTACHMENT

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-
OFFICE OF THE DIRECTOR

SEP 1 0 2002

MEMORANDUM FOR Judith J. Gordon
Assistant Inspector General
for Systems Evaluation

From: Arden L. Bement, Jr.
Director

Subject: Comments on Draft Inspection Report No. OSE-15078, Additional Improvements Needed To Strengthen NIST's Information Security Program

This is in response to your memorandum and draft report dated August 8, 2002, regarding your office's evaluation to determine whether the National Institute of Standards and Technology's (NIST's) information security program for unclassified systems complies with the Government Information Security Reform Act (GISRA). Thank you for the opportunity to review and comment on this draft.

NIST takes seriously the matter of information security and, as indicated in your report, we are taking steps to improve our information security program. During the exit conference following the evaluation, the NIST Deputy Director and Acting Director, Information Technology Laboratory indicated that we agreed generally with your findings and recommendations. I appreciate the work your office has done to highlight these opportunities for improvement, and give you my assurance that we are committed to meeting all GISRA requirements.

The attached comments are intended to clarify statements in the draft report and to update you on actions taken since the completion of your evaluation and issuance of the report.

Thank you, again, for the opportunity to comment on the draft. We are looking forward to receiving and responding to your final report. Please contact Albert Conerly at (301) 975-4050 should you have questions about this response.

Attachment

NIST

ATTACHMENT – Comments to Clarify and Update NIST GISRA Implementation

1. See pages i., 10, 11, and 12 for references to 130 NIST IT Systems, and page 13, **E. System Inventory May Not Reflect Actual Number of Operational Systems.**

Comment: The NIST Systems Inventory currently lists 115 IT systems developed or under development. In May 2002, NIST system owners were to report to the NIST Information Technology Security Office (ITSO) any redefined system boundaries based on additional guidance provided by the ITSO. The additional guidance was reported in scheduled meetings between groups of OU-specific system owners and the ITSO, in OU Computer Security Officer meetings, through email, and on the NIST Computer Security website. In June 2002, the ITSO posted the NIST IT Systems Inventory, which currently contains 109 developed systems, and 6 systems that are under development.

2. See page 6 - **I. NIST Is Taking Steps To Improve Its Information Security Program.**

Comment: Add the following statement to the current last bullet:

- The ITSO also provided a pre-filled 800-26 Self-Assessment Questionnaire Template to NIST Operating Unit (OU) Computer Security Officers on May 3, 2002. During May 2002 Accenture, a NIST contractor, met with system owners to present and explain the questionnaire. A Contingency Plan Template, based on NIST SP 800-34, was provided to OU Security Officers on May 31, 2002, with instructions to complete and return the document by July 26, 2002.

3. See pages 7 and 8 - **A. NIST Lacks A Comprehensive Security Program Policy.**

Comment: NIST has drafted a revision to Chapter 11.02 of the NIST Administrative Manual to include specific roles and responsibilities for NIST Senior Management, including the roles and responsibilities of the NIST Director, NIST CIO, NIST Operating Unit Directors, NIST System Owners, NIST System Administrators, NIST Operating Unit IT Security Officers, NIST IT System Security Officers, and End Users. The draft has been presented to the IT Policy Council and is currently being reviewed and vetted by NIST management.

4. See pages 8 and 9 - **B. Draft Certification and Accreditation Procedures Should Be Strengthened.**

Comment: NIST has modified its draft Certification and Accreditation policy such that NIST Operating Unit Directors will co-accredit Operating Unit IT Systems and the NIST CIO will also co-accredit all NIST IT Systems.

5. See pages 9-11 - **III. Management Controls Are Not Fully Implemented and Schedules Are Unrealistic For Achieving Adequate Product Content and Quality.**

Comment: The Risk Assessment Methodology guidance was delivered to all NIST Operating Units on July 22, 2002. The ITSO changed the Risk Assessment and Accreditation Statements due date to August 23, 2002. Fifty-nine out of 109 system owners met the deadline. The ITSO and NIST CIO are working with other system owners to ensure their Risk Assessment and Accreditation Statements are completed by September 30, 2002. The NIST CIO and the ITSO are tracking the status of systems for which final certification and accreditation documentation has not been submitted. System owners have been informed that uncertified and unaccredited systems will be disconnected from the NIST Network if documentation is not received by September 30, 2002.

For FY2002, the NIST Operating Unit Directors are the accreditation authority. For FY2003, the NIST Operating Unit Directors will co-accredit Operating Unit IT Systems and the NIST CIO will also co-accredit all NIST IT Systems. In addition, in FY2003 the NIST ITSO will conduct an independent review of certified and accredited systems and make recommendations to the NIST CIO.

6. See pages 13 and 14 - **IV. Security Controls Are Not Extended to External Collaborators and Researchers.**

Comment: NIST is addressing the issue as part of an FY2002 Security and Access Control (SAC) project. In FY2001, NIST began the development of a system to better track guest researchers. This system, known as the NIST Associates Information System (NAIS), initially was to track only guest researchers that had a NIST badge, excluding many external collaborators. The SAC efforts changed this to include all guest researchers and external collaborators regardless of whether or not they have a NIST badge. A primary goal for SAC is that all NIST computer accounts will be linked to a central SAC directory. The SAC directory will contain NAIS information, which will include external collaborators, and NIST employee information from the NIST employee database.

7. See page 14 - **V. Risk Levels for Positions Have Not Been Properly Assigned.**

Comment: The NIST CIO has recommended to the NIST Director that all NIST personnel holding system administrator privileges to access any NIST server must have an ADP risk level of either Moderate or High regardless of the percentage of job associated with their server administration work. The NIST Director will issue a memorandum to NIST Operating Units based on this recommendation.

8. See pages 15-17 - **VI. NIST Has Not Implemented a Capital Asset Planning Process.**

Comment: As of June 2002, NIST began implementing a Capital Investment Planning Process as part of its new (FY2002) System Development Life Cycle program in the NIST IT Services area. In addition, as a pilot effort in FY2002, non-services area system owners were instructed to complete and submit to the NIST CIO Office a Capital Investment Plan (an automated template form titled "IT Capital Investment/Business Case Security," provided by the NIST CIO) for any hardware purchases to be made using scientific computing funds. These plans were reviewed by the NIST CIO Support Office, and approved by the NIST CIO, before being processed by the NIST Procurement Office. In FY2003, NIST will fully implement this system across all NIST systems.