IG-00-055

AUDIT REPORT

SYSTEM INFORMATION TECHNOLOGY SECURITY PLANNING

September 28, 2000

National Aeronautics and
Space Administration

OFFICE OF INSPECTOR GENERAL

Additional Copies

To obtain additional copies of this report, contact the Assistant Inspector General for Auditing at (202) 358-1232, or visit www.hq.nasa.gov/office/oig/hq/issuedaudits.html.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Assistant Inspector General for Auditing. Ideas and requests can also be mailed to:

Assistant Inspector General for Auditing
Code W
NASA Headquarters
Washington, DC 20546-0001

NASA Hotline

To report fraud, waste, abuse, or mismanagement contact the NASA Hotline at (800) 424-9183, (800) 535-8134 (TDD), or at www.hq.nasa.gov/office/oig/hq/hotline.html#form; or write to the NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, DC 20026. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.

Reader Survey

Please complete the reader survey at the end of this report or at http://www.hq.nasa.gov/office/oig/hq/audits.html.

Acronyms

ID	Identification
IT	Information Technology
GAO	General Accounting Office
JPL	Jet Propulsion Laboratory
NIST	National Institute of Standards and Technology
NPG	NASA Procedures and Guidelines
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SMA	Special Management Attention

W September 28, 2000

TO: A/Administrator

FROM: WInspector General

SUBJECT: INFORMATION: System Information Technology Security Planning
Report Number IG-00-055

The NASA Office of Inspector General has completed an audit of System Information Technology Security Planning. We found that NASA has not adequately complied with the Computer Security Act of 1987 and Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," dated February 8, 1996. NASA managers did not assign sufficient priority to information technology (IT) security. NASA Headquarters and the Centers had no IT security plans for 17 of 38 special management attention[1] (SMA) systems and for 13 of 30 publicly accessible Web site[2] host computers in our samples. The Jet Propulsion Laboratory (JPL) has no IT security plans for its IT systems. In addition, there are no security plans, contingency plans, or risk assessments for five elements of a major information system.[3] Initial and periodic personnel screening requirements in Agency policy do not comply with OMB Circular A-130 requirements. Therefore, NASA's IT systems are at increased risk and the effectiveness of NASA's IT security program is degraded. The Centers and JPL are working to meet the NASA Chief Information Officer's goal of completing IT security plans for all SMA systems by September 30, 2000. We consider the noncompliance with the Computer Security Act and OMB Circular A-130 to be a potential material management control weakness reportable in accordance with OMB Circular A-123, "Management Accountability and Control," and NASA Policy Directive 1200.1A, "Internal Management Controls, Audit Liaison, and Followup."

---

[1] "Special management attention" is a NASA term for information systems that are considered to be the most important to NASA in accomplishing its mission. Increased oversight of these IT systems is required due to the risk and magnitude of harm that would result from the loss, misuse, unauthorized access to, or modification of the data in a system.

[2] A publicly accessible Web site is one designed to be viewed by the general public. These Web sites are advertised to the public such as, www.nasa.gov, or contain links to other NASA public Web sites.

[3] The system will not be identified in the report due to the sensitivity of this information. However, we have advised NASA officials of the identity of the system so that they may take appropriate corrective action.

Background

NASA is dependent on IT for all its missions and support activities. The integrity, availability, and confidentiality of NASA's electronic information are critically important unless its computing environment is secure. IT security plans report the outcome of the IT security planning process, provide essential information about the system, describe the associated risks, and the security controls that have been implemented. NASA managers must authorize the use of each IT system based on the implementation of its security plan before the system is placed in service, when significant changes are made, and when 3 years have expired since the last authorization.

Recommendations

We recommended that the NASA Chief Information Officer create an inventory containing the status of IT security plans and authorizations to use the systems and require quarterly updates. This inventory will provide senior NASA management more visibility of the status of IT security plans and authorizations to use the systems. NASA managers used a similar inventory during the Year 2000 date conversion problem. We also recommended that Associate Administrators and Center Directors report the Federal noncompliance conditions to the Agency's Internal Control Council[4] as significant areas of concern. Agency managers and employees should identify and report deficiencies that are or should be of interest to the next level of management. We recommended that the Director, Goddard Space Flight Center expedite the development and implementation of IT security plans for one of NASA's major IT systems. IT security plans are the equivalent of Program and Project Plans. Not having a plan significantly increases the possibility that IT security risks have not been identified, adequate protective measures have not been implemented, and NASA managers are unaware of the risks associated with operating the system. Finally, we recommended that the NASA Chief Information Officer expand policy requirements for personnel screenings to comply with OMB Circular A-130. Initial and periodic screening of individuals supplements technical, operational, and management controls, particularly where the risk and magnitude of harm is high.

Management Response and OIG Evaluation

Management concurred with 7 of the 10 recommendations. Management partially concurred with recommendations to report the Federal noncompliance conditions at JPL, Langley Research Center (Langley), and NASA Headquarters to the Agency's Internal Control Council as significant areas of concern. Management stated that Langley and NASA Headquarters are scheduled to have fully compliant IT security plans for all SMA systems by September 30, 2000. With the completion of these plans, there is no need to report noncompliance conditions as a significant area of concern. We agree that there is no need to report the noncompliance

[4] The Internal Control Council makes recommendations to the NASA Administrator on issues for NASA's annual statement of assurance to the President and Congress, pursuant to the Federal Managers' Financial Integrity Act and for incorporation into NASA's annual Accountability Report.

conditions as a significant area of concern, if the noncompliance conditions are corrected by September 30, 2000. However, we have no assurance that Langley and NASA Headquarters will meet the schedules. We have requested that management provide additional information on the completion of SMA system IT security plans at the two locations. In addition, management stated that the condition of IT security plans at JPL is a contractual issue and not a Federal Managers' Financial Integrity Act issue. We agree that JPL does not participate in the Agency's internal control process; however, the NASA officials who manage the programs that JPL conducts do participate. JPL manages a significant amount of IT resources that are essential to the conduct of Agency programs. NASA managers are ultimately responsible for the security of NASA's IT resources. We have asked that management reconsider its position on the reporting of significant areas of management concern related to functions performed by contractors.

[original signed by]
Roberta L. Gross

Enclosure
Final Report on Audit of System Information Technology Security Planning

FINAL REPORT
SYSTEM INFORMATION TECHNOLOGY SECURITY PLANNING

W September 28, 2000

TO: AO/Chief Information Officer

FROM: W/Assistant Inspector General for Auditing

SUBJECT: Final Report on the Audit of System Information Technology Security Planning
Assignment Number A0003700
Report Number IG-00-055

The subject final report is provided for your information and use. Please refer to the Executive Summary for the overall audit results. Our evaluation of your responses has been incorporated into the body of the report. The corrective actions taken or planned for recommendations 1, 2, 5, 6, 7, 9, and 10 are responsive. The corrective actions planned for recommendations 3, 4 and 8 are not responsive because additional information is needed for us to determine whether management has corrected the Federal noncompliance conditions related to the recommendations. In addition, we request that management reconsider its position on recommendation 4 concerning reporting of significant areas of management concern. Your actions are sufficient to close recommendations 2, 5, and 6 for reporting purposes. We request additional information as described in the report for recommendations 1, 3, 4, and 8 by November 27, 2000. Recommendations 1, 7, 9, 10 will remain open for reporting purposes until agreed-to corrective actions are completed. For corrective actions that are incomplete, please notify us when action has been taken, including the extent of testing performed to ensure corrective actions are effective.

If you have questions concerning the report, please contact Mr. Gregory B. Melson, Program Director, Information Assurance Audits, at (202) 358-2588, or Mr James W. Geith, Auditor-in-Charge, at (301) 286-7943. We appreciate the courtesies extended to the audit staff. The final report distribution is in Appendix E.

[Original signed by]

Russell A. Rau

Enclosure

cc:
B/Chief Financial Officer
B/Comptroller
BF/Director, Financial Management Division
C/Associate Administrator for Headquarters Operations
G/General Counsel
H/Associate Administrator for Procurement
M/Associate Administrator for Space Flight
R/Associate Administrator for Aerospace Technology
S/Associate Administrator for Space Science
Y/Associate Administrator for Earth Science
JM/Acting Director, Management Assessment Division
GRC/3-2/Director, John H. Glenn Research Center at Lewis Field
GSFC/100/Director, Goddard Space Flight Center
JPL/1000/Director, Jet Propulsion Laboratory
LaRC/106/Director, Langley Research Center

Contents

NASA Office of Inspector General

IG-00-055 **September 28, 2000**
A0003700

System Information Technology Security Planning

Executive Summary

Background. Successful accomplishment of NASA's mission depends heavily on automated information resources. As technology evolves, these resources face increasing vulnerability to external and internal attack. Our risk-based analysis of various Federal IT security requirements indicated that NASA's IT security planning was the most fundamental and highest risk area for which additional NASA Office of Inspector General review was warranted. Specifically, we determined that a review of strategic and system information security planning, including the adequacy of existing policy and implementation, should be the first step in assessing NASA-wide information security activities.[5]

Objectives. The overall objective was to determine whether NASA had established and implemented effective security plans for general support systems[6] and major applications,[7] including publicly accessible Web sites. We reviewed a sample of 38 IT security plans for SMA IT systems and a sample of 30 plans for computers that host publicly accessible Web sites[8] at eight NASA

---

[5] The General Accounting Office (GAO) stated in its Report Number GAO/AIMD-98-68, "GAO Executive Guide, Information Security Management, Learning from Leading Organizations," May 1998:

> The single most important factor in prompting the establishment of an effective security program was a general recognition and understanding among the organization's most senior executives of the enormous risks to business operations associated with relying on automated and highly interconnected systems. However, risk assessments of individual business applications provided the basis for establishing policies and selecting related controls. Steps were then taken to increase the awareness of users concerning these risks and related policies. The effectiveness of controls and awareness activities was then monitored through various analyses, evaluations, and audits, and the results provided input to subsequent risk assessments, which determined if existing policies and controls needed to be modified.

[6] OMB Circular A-130 defines a general support system as "an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people."

[7] OMB Circular A-130 defines a major application as "an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application."

[8] We identified a universe of 177 security plans for SMA IT systems and a universe of 195 security plans for Web site host computers.

installations.[9] We compared the contents of the security plans with the requirements for security plans in OMB Circular A-130 and NASA Procedures and Guidelines (NPG) 2810.1, "Security of Information Technology," dated August 26, 1999. Details on our objectives, scope, and methodology are in Appendix A.

Results of Audit. NASA has not adequately complied with the Computer Security Act of 1987 and OMB Circular A-130.

- NASA Headquarters and the Centers had no IT security plans for 17 of 38 SMA systems and for 13 of 30 Web site host computers in our samples. JPL has no IT security plans for its IT systems. None of the IT security plans in either sample fully complies with OMB Circular A-130. In addition, there are no security plans, contingency plans, or risk assessments for five major elements of a major information system. The lack of adequate IT security plans significantly reduces the effectiveness of the IT security programs for those systems. The Centers and JPL intend to complete the IT security plans for SMA systems by September 30, 2000 (Finding A).

- Initial and periodic personnel screening requirements in NPG 2810.1 do not comply with OMB Circular A-130 requirements. The NPG lacks requirements for periodic screening of individuals authorized to bypass system security controls. In addition, the NPG lacks a requirement to use initial and periodic personnel screening as a control when applications or the information in an application cannot be adequately protected because line managers do not use other controls such as individual accountability or when the controls do not provide sufficient protection. Inadequate personnel screening combined with the use of group user ID's increased the security risks for IT systems (Finding B).

We consider the Agency noncompliance with the Computer Security Act and OMB Circular A-130 to be a potential material control weakness reportable in accordance with OMB Circular A-123, "Management Accountability and Control," June 21, 1995, and NASA Policy Directive 1200.1A, "Internal Management Controls, Audit Liaison, and Followup," dated June 1, 2000 (see Appendix C for a detailed discussion).

Recommendations. We recommended that NASA management establish an inventory of IT systems and IT security plans to manage the development and implementation of IT system security programs, develop and implement IT security plans for some elements of a major IT system, and revise Agency IT security policy on personnel screening requirements. Also, Associate Administrators and Center Directors should report to the Agency's Internal Control Council the Federal noncompliance conditions as significant areas of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

[9] We reviewed security plans at NASA Headquarters, Ames Research Center (Ames), John H. Glenn Research Center at Lewis Field (Glenn), Goddard Space Flight Center (Goddard), John F. Kennedy Space Center (Kennedy), Lyndon B. Johnson Space Center (Johnson), Langley, and George C. Marshall Space Flight Center (Marshall).

Management's Response. Management concurred with the recommendations to establish an inventory of IT systems and IT security plans, to develop and implement IT security plans for some elements of a major IT system, and to revise Agency IT security policy on personnel screening requirements. The Director, Glenn Research Center at Lewis Field and the Director, Goddard Space Flight Center concurred with the recommendations to report their respective Center's Federal noncompliance conditions as a significant area of concern to the Agency's Internal Control Council. The Associate Administrator for Headquarters Operations, the Associate Administrator for Space Science, and the Director, Langley Research Center partially concurred with these recommendations. Langley and NASA Headquarters have scheduled completion all of their SMA system IT security plans by September 30, 2000. Management stated that if all the plans are completed, the noncompliances would no longer exist, and there would be nothing to report. In addition, the Associate Administrator for Space Science did not agree on the applicability of OMB Circular A-123 reporting requirements to JPL's operations.

Evaluation of Management's Response. Management's planned or completed actions on the recommendations to establish an inventory of IT systems and IT security plans, to develop and implement IT security plans for some elements of a major IT system, and to revise Agency IT security policy on personnel screening requirements are responsive. The Center Directors' reporting of their Center's Federal noncompliance conditions as a significant area of concern was also responsive. The responses by the Associate Administrator for Headquarters Operations, and the Director, Langley Research Center are not fully responsive without evidence that shows the significant noncompliance conditions we found no longer exist. The Associate Administrator for Space Science's position on reporting management concerns related to JPL's operations is nonresponsive because NASA managers are ultimately responsible. We request that we be notified when the SMA system IT security plans for the IT systems at Langley and NASA Headquarters are completed so that we can review them. We also request that the Associate Administrator for Space Science reconsider his position on reporting JPL's Federal noncompliance conditions as a significant area of concern to the Internal Control Council.

Introduction

The current NASA Strategic Plan states that one of NASA's objectives is to:

> Ensure information technology provides an open and secure exchange of information, is consistent with Agency technical architectures and standards, demonstrates a projected return on investment, reduces risk, and directly contributes to mission success.

To achieve the objective of security in computing, NASA must ensure that the following three computer security characteristics are maintained:

a. Integrity--The ability to ensure that information, the applications processing that information, the information technology systems used to run that information, and the hardware configuration, connectivity, and the status of privilege settings cannot be altered during processing, storage or transmission.

b. Availability--The ability to ensure that data, applications, and systems are accessible when and where needed.

c. Confidentiality--The ability to ensure that information is disclosed only to those who have a valid need to possess it.

A secure computing environment is based on managing the risks to an appropriate level. The security controls applied to a computer system should be commensurate with the magnitude of harm that would result from the loss, misuse, inability to access, unauthorized access to, or modification of the information in the system. An IT security plan reports the outcome of the IT security planning process. An IT security plan provides key information about the system and describes the associated risks and the security controls that have been implemented. The IT security plan is the source document that describes how the security controls for a particular system function.

The NASA Administrator recently emphasized the importance of IT security planning in his Safety and Health Message, titled "NASA Security: Classified Information, Information Technology, and International Technology Transfer/Export Controls," dated June 19, 2000. The Administrator stated:

> Every NASA information technology system must have a security plan that included risk assessment and implementation of appropriate safeguards. These plans must be signed by the project or program manager to attest that the system is ready to operate.

Findings and Recommendations

Finding A. System Security Controls

NASA managers have not developed and implemented IT security plans for many of the Agency's SMA IT systems and computers that host publicly accessible Web sites. In addition, many of the existing IT security plans are inadequate, and several of NASA's SMA IT systems and Web site host computers are operating without the required authorizations. These conditions exist because NASA managers have not complied with Federal policy and have given IT security a low priority. Consequently, the security risks have increased for many SMA IT systems and other IT resources and the effectiveness of NASA's IT security program has been reduced. We consider the noncompliance with the Computer Security Act and OMB Circular A-130 to be a potential material weakness reportable to the Agency's Internal Control Council.

Federal Policies on Information Technology Security Planning

"The Computer Security Act of 1987," Public Law 100-235, requires agencies to establish a security plan for each Federal computer system.

OMB Circular A-130, Appendix III, requires that agencies implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in IT systems. The Circular identifies four controls that are required for each IT system. Agency managers must:

- Assign responsibility for the security of each system to an individual knowledgeable in the information technology used in the system and in providing security for such technology.

- Plan for adequate security of each general support system and major application. Each security plan must contain the information required by the Circular.

- Review the security controls in each system when significant modifications are made to the system or when 3 years have elapsed since the last review.

- Authorize in writing the use of each system based on the implementation of its security plan before beginning or significantly changing processing in the system. Authorizations to process must be renewed at least every 3 years.

The Circular also requires that IT security plans establish system requirements for a number of controls for general support systems, including:

- Rules of the System. The plan must establish a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system. The rules must clearly describe the consequences of behavior not consistent with the rules.

- Training. The plan must describe how all individuals will be trained in how to fulfill their security responsibilities before allowing them access to the system. Behavior consistent with the rules of the system and periodic refresher training must be required for continued access to the system.

- Personnel Controls. The plan must require screening of individuals who are authorized to bypass significant system technical and operational security controls of the system commensurate with the risk and magnitude of harm these individuals could cause. Such screening shall occur before an individual is authorized to bypass controls and periodically thereafter.

- Incident Response Capability. The plan must describe the capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations, consistent with National Institute of Standards and Technology (NIST) coordination, and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.

- Continuity of Support. The plan must establish the capability to continue providing service within a system based upon the needs and priorities of the participants of the system. The plan must include requirements for periodically testing the capability.

- Technical Security. The plan must describe how cost-effective security products and techniques are appropriately used within the system.

- System Interconnection. The plan must include the requirement to obtain written management authorization, based upon the acceptance of risk to the system, before connecting with other systems.

Circular A-130 establishes similar requirements for security plans for major applications. (Appendix B contains the detailed requirements.)

NASA Policies on Information Technology Security Planning

NPG 2810.1 implements the Computer Security Act and Circular A-130 requirements. The Circular requires only that a responsible manager sign the authorization to use the system. The NPG adds a requirement that the Center Chief Information Officer also sign the authorization to use for SMA systems.

Information Technology Security Plans

We used a combination of random and judgmental sampling to select a sample of IT security plans for 38 SMA systems and 30 Web site host computers at 8 NASA Centers. There were no IT security plans for 17 of the SMA systems and for 13 of the Web site host computers. At Glenn, NASA Headquarters, and Langley, none of the sampled SMA IT systems had a security plan. Only

one of the five Web site host computers in the Glenn sample had a security plan. The sampled Web site host computers at NASA Headquarters and Langley had no IT security plans. We did not review a sample of IT security plans at JPL because we determined during our initial data gathering that JPL had no security plans for any of its IT systems.

Major System IT Security Planning. One of NASA's five major IT investments is a system that is composed of 14 elements. We included the system in the group of systems that had security plans because we reviewed a security plan for one of the elements. However, there were no security plans, contingency plans, or current risk assessments for five of the major elements as required by the system's "Security Policy and Guidelines," dated October 1997.

Compliance with Federal and Agency Policy

IT Security Plan Compliance with OMB Circular A-130. Deficiencies existed in IT security plans because line managers either did not establish required security controls or did not document the security controls in the plans. None of the 21 existing SMA system IT security plans and none of the 17 existing IT security plans for the Web site host computers fully complied with Circular A-130 requirements. While some plans lacked information in one or two areas, most of the plans lacked information for several of the controls required by the Circular. Common problems involved the lack of information on system rules of behavior, initial and periodic training, personnel controls, identifying and reporting security incidents, continuity of service, technical security, and system interconnection (see Appendix B). Some of this information existed in other documents that were not referenced in the security plans. For example, many systems had system rules of behavior, contingency plans, and procedures for identifying and reporting security incidents in various documents that are not part of the security plan.

IT Security Plan Compliance with NPG 2810.1. Only 9 of the 21 existing SMA system IT security plans and 9 of the 17 existing IT security plans for Web site host computers have been updated based on the requirements of NPG 2810.1. None of the plans contained all the information required by the NPG. While the deficiencies varied from plan to plan, many plans lacked information on rules of the system or application, contingency planning, training, and procedures for reviewing security controls. Civil service and contractor personnel who rewrote the security plans using NPG 2810.1 criteria did not include all the required information. In addition, NASA management approved the plans but did not determine that required information was missing.

Authorizations to Process

NASA managers had authorized only 12 of the 38 SMA systems and 16 of the 30 Web site host computers in the sample to operate. The authorizations for one SMA system and one Web site host computer had expired. Although there were no security plans, the NASA managers responsible for three of the elements of a major IT system signed authorizations to process. Center Chief Information Officers had not signed 11 of the authorizations to process that were prepared after NPG 2810.1 became effective.

The General Accounting Office (GAO) reported the failure of NASA managers to complete required authorizations for IT systems in its audit report titled, "Information Security, Many NASA Mission-Critical Systems Face Serious Risks," Report Number GAO/AIMD-99-47, May 1999. The GAO report states that NASA managers had not authorized the use of 133 of the 155 systems in the GAO sample. NASA concurred with the GAO recommendation to implement an effective IT security program that includes formally authorizing the use of all systems before they become operational and at least every 3 years thereafter. NASA management included the requirement in NPG 2810, which was issued August 26, 1999.

Priority of Information Security

The absence and inadequacy of security plans and lack of authorizations to process resulted from the low priority that NASA managers consistently gave to IT security and compliance with the Computer Security Act, OMB Circular A-130, and NPG 2810.1. In addition, many IT security plans do not comply with Circular A-130 because Center and Program managers continued to use the outdated guidance in NASA Handbook 2401.9A, "NASA Automated Information Security," dated June 1993, to manage their IT security programs until NPG 2810.1 was issued. The NASA Handbook required security plans for each IT system and that NASA managers authorize the use of the system at least every 3 years or more often if major changes were made to the system. The NASA Handbook did not require that the security plans contain some of the information required by OMB Circular A-130. Security plans that were rewritten using the NPG 2810.1 requirements lacked information required by OMB Circular A-130 because the NPG initial and periodic personnel screening requirements for IT security plans do not comply with OMB Circular A-130 (see Finding B).

The lack of IT security plans for the major IT system elements can also be attributed to the low priority the Project Office gave IT security. The Project Office planned to have the development contractor prepare the plans and risk assessments, but the requirement was not included in the contract because of problems in the development of the system. Extensive modifications to the planned system were needed. NASA managers directed the contractor to concentrate its efforts on the modification of the system.

Management Controls

Information technology security policies and plans are part of the management controls for IT resources. If an agency has no security plan or required authorization to process for a system, OMB Circular A-130 requires that the agency consider identifying a deficiency pursuant to OMB Circular A-123 and the Federal Managers' Financial Integrity Act. Additionally, NASA Policy Directive 1200.1A, "Internal Management Controls and Audit Liaison and Followup," requires managers to identify and recommend significant areas of concern that may be the result of weak, inadequate, or unenforced management controls. The management control officer will determine whether significant areas of concern are reported. The widespread noncompliance with the Computer Security Act, OMB Circular A-130, and NPG 2810.1 reported in this report and GAO Report Number GAO/AIMD-99-47 indicates that many of NASA's management controls related to IT security are

inadequate and unenforced. Yet, only the Director, Goddard Space Flight Center, identified IT security as a significant weakness and concern during fiscal year 1999. (See Appendix C for a detailed discussion on the procedures for reporting significant areas of concern.)

Effect on NASA's IT Security Program

The absence and inadequacy of security plans for many IT systems and the lack of authorizations to process significantly degrade the security of the SMA systems and Web site host computers. The effectiveness of the NASA IT security program has been significantly reduced.

Management Actions

NASA management increased emphasis on IT security in 1998. NASA management was aware of noncompliances with Federal and Agency IT security policy, procedures, and guidelines. The NASA Chief Information Officer established a goal of completing IT security plans for all SMA systems by September 30, 2000. In response, Glenn, Headquarters, JPL, Langley, and most of the other Centers are developing or revising IT security plans using the NPG 2810.1 guidelines and intend to complete the security plans for SMA systems by September 30, 2000. However, the Agency has not modified many IT services contracts to require compliance with the NPG. For example, Johnson has not modified Consolidated Space Operations Contract NAS9-98100 to require preparation of information security plans that comply with the NPG. This contract supports the IT resources that support space operations at Goddard, JPL, Johnson, Kennedy, and Marshall. In addition, Goddard intends to update its plans as they come up for the 3-year review. On July 14, 2000, the NASA Office of Procurement issued Procurement Information Circular 00-12. This Procurement Information Circular establishes standard contractual requirements for safeguarding the integrity of unclassified NASA information technology systems. The Circular requires that contracting officers add a revised NASA Federal Acquisition Regulation Supplement clause to all existing solicitations and contracts by December 31, 2000, where appropriate. The clause requires that NASA contractors and subcontractors comply with the security requirements outlined in NASA Policy Directive 2810.1, "Security of Information Technology," dated October 1, 1998, and NPG 2810.1 and with additional safeguarding requirements in the contract clause.

Glenn expects to complete 25 percent of its Web site IT security plans by October 2000. While JPL has not established specific completion dates for its Web site IT security plans, JPL management estimates it will complete all of its IT security plans by September 30, 2001. Headquarters expects to complete all of its Web site IT security plans by April 30, 2001. As a result, some Web site IT security plans may not comply with OMB Circular A-130 until 2002 or later.

Model of Meeting Year 2000 Date Conversion Problem to Develop and Implement Security Plans

When NASA faced the Year 2000 date conversion problem, the NASA Chief Information Officer created an Agency-wide inventory of IT systems. The inventory indicated whether the system was Year 2000 compliant and showed schedule information for the actions being taken to make noncompliant systems compliant. The NASA Centers submitted quarterly reports that identified their progress in fixing the noncompliant systems. This process proved to be effective for managing the Year 2000 date conversion problem and could be equally effective for managing the development and implementation of IT security plans. Note, however, there is not a one-to-one correlation between the number of IT systems and the number of security plans that are required. For some systems, NASA management has chosen to develop separate security programs for each major element or component of the system. This separation of security responsibility would make it necessary for the inventory to identify the status of the security plans and authorizations to process for each element.

Recommendations, Management's Response, and Evaluation of Response

The NASA Chief Information Officer should:

1. Create of an inventory of every NASA IT system and the status of the supporting IT security plans and required authorizations to process. The inventory should identify those systems for which NASA management will have separate security plans for each major element or component of the IT system.

Management's Response. Concur. The Chief Information Officer's staff will maintain an SMA systems inventory from data the Centers provide. The Centers will maintain inventories of other IT systems. The Agency Chief Information Officer's staff will be able to access the inventories.

Evaluation of Management's Response. Management's proposed actions are responsive to the recommendation. The recommendation is resolved but will remain undispositioned and open until agreed-to corrective actions are completed. We request that management provide a schedule for establishing the inventories.

2. Require the Centers and the Jet Propulsion Laboratory to submit quarterly status reports until there is a current security plan and authorization to process for each IT system or system element.

Management's Response. Concur. The Chief Information Officer requires a quarterly status report on priority systems. The Chief Information Officer determines each year what the priority systems will be. For FY 2000, the Chief Information Officer defined the priority systems as SMA systems.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved and dispositioned.

3. The Associate Administrator for Headquarters Operations should report to the Agency's Internal Control Council the Headquarters' Federal noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

Management's Response. Partially concur. NASA Headquarters has developed a schedule to correct the deficiencies that were noted at the time of the audit. All SMA systems are scheduled to have fully compliant IT security plans with Chief Information Officer approval by September 30, 2000. All Headquarters general support systems will have IT security plans by April 30, 2001. With the completion of these plans, there is no need to report noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

Evaluation of Management's Response. Management is not fully responsive to the recommendation. We agree that there is no need to report the noncompliance conditions if NASA Headquarters corrects the deficiencies by September 30, 2000. However, NASA management has not provided evidence to show that the significant noncompliance conditions we found no longer exist. Therefore, the recommendation is unresolved and undispositioned. We request that we be notified when management completes the SMA system IT security plans so that we can review them.

4. The Associate Administrator for Space Science should report to the Agency's Internal Control Council the Jet Propulsion Laboratory Federal noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

Management's Response. Partially concur. Management agrees that JPL should have IT security plans. However, this is a contractual issue and not a Federal Managers' Financial Integrity Act issue. Because of JPL's status as a contractor-operated installation, JPL does not participate in the Agency's internal control process. The Agency's contractual relationship with the California Institute of Technology, which manages JPL, provides for assessments of contractor performance through the mechanism of semiannual performance evaluations.

Evaluation of Management's Response. Management's comments are not responsive to the recommendation. We recognize that JPL is a contractor and does not participate in the Agency's internal control process. The NASA officials who manage the programs that JPL conducts do participate in the Agency's internal control process and are required to report significant areas of concern for their area of responsibility. JPL manages a significant amount of NASA's IT resources. The logical extension of management's position is that no deficiencies in any of NASA's IT systems that are managed by contractors are reportable. This is not the case. OMB Circular A-130 and NPG 2810.1 hold NASA managers responsible for

the security of Government information technology systems. We request that management reconsider its position and provide additional comments. The recommendation is unresolved and undispositioned.

5. The Director, John H. Glenn Research Center at Lewis Field, should report to the Associate Administrator for Aerospace Technology the Glenn Federal noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

Management's Response. Concur. Glenn has already reported this condition in its August 15, 2000, Federal Managers' Financial Integrity Act annual statement of assurance. Glenn has a project plan in place to complete all of its SMA system IT security plans by September 30, 2000, and all the remaining IT system security plans by September 30, 2002.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved and dispositioned.

The Director, Goddard Space Flight Center, should:

6. Report to the Associate Administrator for Earth Science the major IT system Federal noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

Management's Response. Concur. The Director's Statement of Assurance to the Associate Administrator for Earth Science highlights IT security as one of three areas for special discussion. The Statement of Assurance discusses many actions that Goddard is taking to improve IT security. These actions include addressing, in particular, the IT security issues identified in this report.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved and dispositioned.

7. Expedite the development and implementation of the required security plans, contingency plans, and risk assessments for the major IT system.

Management's Response. Concur. Each of the specified elements of this major information system will deliver a comprehensive security plan, contingency plan, and risk assessment to the major element IT Security Official by the end of the calendar year. The major element IT Security Official will present these plans and assessments to the Goddard Chief Information Officer for his review.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved but will remain undispositioned and open until agreed-to corrective actions are completed.

8. The Director, Langley Research Center, should report to the Associate Administrator for Aerospace Technology the Langley Federal noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

Management's Response. Partially concur. All Langley SMA system plans are scheduled for completion by September 30, 2000. With the completion of these plans, there is no need to report noncompliance conditions as a significant concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

Evaluation of Management's Response. Management is not fully responsive to the recommendation. As stated in our response to management's comments on recommendation 3, we agree that there is no need to report the noncompliance conditions if Langley corrects the deficiencies by September 30, 2000. However, NASA management has not provided evidence that shows the significant noncompliance conditions we found no longer exist. Therefore, the recommendation is unresolved and undispositioned. We request that we be notified when management completes the SMA IT security plans so that we can review them.

Finding B. Personnel Screening

The personnel screening requirements in NPG 2810.1 do not comply with OMB Circular A-130. The NPG does not require periodic screening of individuals who can bypass system security controls or initial and periodic screening of individuals when applications or the information in the application are not adequately protected because managers did not use other controls, such as, individual accountability or when the controls do not provide adequate security for mission information systems.[10] This occurred because NASA management overlooked the Circular A-130 requirements when it developed and approved the NPG. As a result, the security of all NASA IT systems may be degraded.

Federal Policies and Procedures

OMB Circular A-130, Appendix III, requires that security plans for general support IT systems (see details in footnote 6) include screening individuals who are authorized to bypass significant technical and operational security controls of a system commensurate with the risk and magnitude of harm these individuals could cause. Such screening shall occur before an individual is authorized to bypass controls and periodically thereafter.

OMB Circular A-130, Appendix III, also requires that IT security plans for major applications (see details in footnote 7) incorporate controls such as separation of duties, least privilege[11] and individual accountability into the application and application rules of behavior, as appropriate. When such controls cannot adequately protect the application or information in the application, individuals should be screened commensurate with the risk and magnitude of the harm they could cause. Such screening shall be done before an individual is authorized to access the application and periodically thereafter.

Existing NASA Policy

NPG 2810.1 does not adequately address the personnel screening requirements in OMB Circular A-130. The NPG requires an initial screening of individuals who are authorized to bypass significant technical and operational controls of IT systems, but does not require additional periodic screening. Further, the NPG does not require managers to require initial and periodic screening of individuals when applications or the information in the application are not adequately protected because line managers did not use other controls such as individual accountability or the controls do not provide sufficient protection.

Personnel screening is particularly important because NASA does not always use individual accountability as a system control. Appendix A of the NPG discourages but permits the use of

[10] Mission information systems contain information, software applications, or computer systems that if altered, destroyed, or unavailable, could have a catastrophic effect on NASA. Mission information systems include systems that control or directly support human space flight and space vehicle operations.

[11] Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (for example read, write, execute, delete) to the minimum necessary to perform his or her job.

group user ID's on all categories of information systems, including mission information systems. When an individual logs on[12] to a system using a group user ID,[13] the system has no way of determining a specific individual. Consequently, individual accountability is lost for that session. During this and previous audit work, we identified two mission information systems that are using group user ID's. One system supports human space flight; the other system supports space vehicle operations. The daily use of group user ID's is a significant security risk that degrades the security of mission systems.

Recommendations for Corrective Action

The NASA Chief Information Officer should revise NPG 2810.1 to comply with OMB Circular A-130 requirements. Specifically, the NPG should be revised to require:

9. Periodic screening of individuals who are authorized to bypass significant technical and operational controls of IT systems.

Management's Response. Concur. Compliance with OMB A-130 will be addressed in the next revision of NPG 2810.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved but will remain undispositioned and open until agreed-to corrective actions are completed.

10. Initial and periodic screening of all individuals commensurate with the risk and magnitude of the harm they could cause when applications or the information in the application are not adequately protected because line managers did not use other controls such as individual accountability or the controls do not provide sufficient protection.

Management's Response. Concur. Compliance with OMB A-130 will be addressed in the next revision of NPG 2810.

Evaluation of Management's Response. Management's actions are responsive to the recommendation. The recommendation is resolved but will remain undispositioned and open until agreed-to corrective actions are completed.

[12] NPG 2810.1 defines logon as "the identification and authentication sequence that authorizes a user's access to the system."
[13] A group user identification is a system identification that is shared among a group of individuals for logging in to a computer, application, or set of files.

Appendix A. Objectives, Scope, and Methodology

Objectives

The overall objective was to determine whether NASA has established and implemented effective policies and procedures for IT security planning in accordance with OMB Circular A-130. Specifically, we determined whether the Agency has developed adequate security plans for general support IT systems, major applications, and publicly accessible Web sites (see details on these systems in footnotes 6, 7, and 2).

We announced that we would also determine whether the Agency established effective IT security planning processes as an integral part of its strategic information resources management program.[14] The audit announcement stated that we will review the:

- IT security planning metrics developed for reporting under the Government Performance and Results Act;

- management actions taken on the recommendations from the GAO report number GAO/AIMD-99-47, "Information Security, Many NASA Mission-Critical Systems Face Serious Risks"; and

- management actions taken on the recommendations from NASA's internal "Information Technology Security Program Review."

We will cover these elements in the next phase of continuing audit field work and will address them in a subsequent report(s).

Scope

We performed work at NASA Headquarters, Ames, Glenn, Goddard, JPL, Kennedy, Johnson, Langley, and Marshall. We reviewed a sample of 38 IT system security plans for SMA systems and a sample of 30 IT system security plans for computers that host publicly accessible Web sites. We interviewed NASA and contractor personnel to identify policies and procedures related to IT security planning and authorizations to process. We also reviewed IT system security plans to determine whether the plans contained the information required by OMB Circular A-130. We determined whether each IT system in our samples had a current authorization to process. We did not perform detailed testing to determine the adequacy or effectiveness of the security measures or the accuracy of the information in each IT system security plan. We did not use computer-processed data in the audit.

[14] The audit announcement stated that we would determine whether the Agency has implemented an adequate strategic information resources management plan that incorporates the system security plans for general support systems and major applications. We cancelled this objective because the underlying requirement has been deleted by the Information Technology Reform Act of 1996.

Appendix A

We are separately reviewing NASA's implementation of Presidential Decision Directive 63, "Protecting American's Critical Infrastructures," dated May 22, 1998, under audit assignment A0003200, "Review of NASA's Planning and Implementation for Presidential Decision Directive 63." The objectives of this review are to determine whether NASA has developed an effective plan for protecting its critical cyber-based infrastructure, identified its critical assets, and adequately assessed vulnerabilities.

Methodology

We developed two universes of IT system security plans. The first universe consisted of the system security plans for the SMA IT systems at eight audit locations, which are listed in the table that follows this section. The second universe consisted of the IT system security plans for the computers at the eight audit locations that hosted publicly accessible Web sites. We used random sampling to select five IT system security plans for SMA systems and five security plans for computers that hosted publicly accessible Web sites at each of the eight audit locations. When there were fewer than five IT security plans for Web site host computers at a location, we reviewed all the plans. We intended to review a sample of the IT security plans at JPL, but we learned during the initial data gathering process that JPL had no security plans for any of its IT systems.

Some Centers identified the security plans for each SMA system and Web site host computer. When Centers did not identify the IT security plans for their systems, we assumed there was one IT security plan for each SMA system and one IT security plan for each Web site host computer. After we started the field work, we learned that some SMA systems had several security plans. Each plan covered one or more of the system elements. When this situation occurred, we judgmentally selected one of the plans for review. For example, the Space Network Systems at Goddard has three IT security plans that cover four major components. We selected the security plan for the Network Control Center for review.

The table below shows the number of sampled IT security plans relative to the universe of SMA systems and Web site host computers.

Center	Number of Plans[1]		Plans Sampled	
	SMA Systems	Web Site Host Computers	SMA	Web Site Host Computers
Ames	6	24	5	7[2]
Goddard	32	60	5[3]	5
Glenn	17	34	5	5
Headquarters	14	14	5	5
Johnson	23	25	5	0[5]
Kennedy	17	34	5	4[4]
Langley	31	1	5	1
Marshall	37	3	3[5]	3
Total	177	195	38	30

[1] There is no direct correlation between the number of IT security plans and the number of SMA systems or Web site host computers. Some IT security plans covered more than one SMA system or Web site host computer. Three of the SMA systems in the samples had several security plans. Because we did not make additional inquiries for each system, there may be more SMA IT security plans than shown in the table.

[2] We judgmentally added two more Web site host computers to the sample at Ames because of the large number of Web sites on the computers.

[3] After we started our field work, we learned that there was more than one IT system security plan for three of the SMA systems in our Goddard sample. We judgmentally selected one of the plans for each system for review.

[4] We initially selected a sample of five Web site host computer IT system security plans. Kennedy had difficulty in locating one of the plans. After we completed our visit to Kennedy, we learned that two of the Web sites were on the same computer. Therefore, we reduced the sample size for Kennedy.

[5] We reduced the sample due to resource and time constraints.

Management Controls Reviewed

We reviewed Federal and NASA policies and procedures relating to IT security planning to determine whether NASA's IT security policies and system security plans were adequate. We identified a potential material management control weakness (Finding A) and other management control weaknesses (Finding B), which are discussed in the Findings section of the report.

Appendix A

Audit Field Work

We performed field work from March through July 2000 at NASA Headquarters, Ames, Glenn, Goddard, Johnson, Langley, Kennedy, and Marshall. We performed the audit in accordance with generally accepted auditing standards. In addition, we collected information from JPL.

Prior Audit Coverage

The GAO issued an audit report titled "Information Security, Many NASA Mission-Critical Systems Face Serious Risks," Report Number GAO/AIMD-99-47, May 1999. The GAO found that NASA was not effectively and consistently managing IT security throughout the agency. NASA's IT security program did not include key elements of a comprehensive IT security management program. Specifically, NASA:

- did not effectively assess risks or evaluate needs. One hundred thirty-five of the 155 mission-critical systems that we reviewed did not meet all of NASA's requirements for risk assessments.

- did not effectively implement policies and controls. NASA's guidance did not specify what information can be posted on public World Wide Web sites nor how mission-critical systems should be protected from well-known Internet threats.

- was not monitoring policy compliance or the effectiveness of controls. NASA had not conducted an agency-wide review of IT security at its 10 field centers since 1991. Furthermore, the security of 60 percent of the systems that we reviewed had not been independently audited.

- was not providing required computer security training. NASA had no structured security training curriculum.

- did not centrally coordinate responses to security incidents. NASA field centers were not reporting incidents to the NASA Automated Systems Incident Response Capability.

NASA management is aware that its IT security program needs improvement. Accordingly, in May 1998 NASA initiated a special review of its IT security program. The review identified a number of shortcomings that were consistent with our findings. Although NASA is planning to address these shortcomings, at the time of our review, few of the special review's recommendations had been implemented.

Appendix B. Federal Guidance on Information Technology Security

OMB Circular A-130, "Management of Federal Information Resources." Circular A-130 provides uniform management policies on Governmentwide information resources. Appendix III of the Circular establishes a minimum set of controls to be included in Federal automated information security programs.

OMB Circular A-130, Appendix III, paragraph A.3.a., requires that agency programs include the following controls in their general-support systems and major applications:

> a. Controls for general support systems.
>
> 1) Assign responsibility for security in each system to an individual knowledgeable in the IT used in the system and in providing security for such technology.
>
> 2) Plan for adequate security of each general support system as part of the organization's information resources management (IRM) planning process. Security plans shall include:
>
> a) Rules of the System. Establish a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system. The rules shall be based on the needs of the various users of the system. The rules shall be only as stringent as necessary to provide adequate security for information in the system. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system. They shall also include appropriate limits on interconnections to other systems and shall define service provision and restoration priorities. Finally, they shall be clear about the consequences of behavior not consistent with the rules.
>
> b) Training. Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM [Office of Personnel Management]. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system.
>
> c) Personnel Controls. Screen individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause. Such screening shall occur before an individual is authorized to bypass controls and periodically thereafter.

d) Incident Response Capability. Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations, consistent with NIST coordination, and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.

e) Continuity of Support. Establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system.

f) Technical Security. Ensure that cost-effective security products and techniques are appropriately used within the system.

g) System Interconnection. Obtain written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems. Where connection is authorized, controls shall be established which are consistent with the rules of the system and in accordance with guidance from NIST.

3) Review of Security Controls. Review the 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 system. Depending on the potential risk and magnitude of harm that could occur, consider identifying a deficiency pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act (FMFIA), if there is no assignment of security responsibility, no security plan, or no authorization to process for a system.

4) Authorize Processing. Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years.

b. Controls for Major Applications.

1) Assign Responsibility for Security. Assign responsibility for security of each major application to a management official knowledgeable in the nature of the information and process supported by the application and in the management, personnel,

operational, and technical controls used to protect it. This official shall assure that effective security products and techniques are appropriately used in the application and shall be contacted when a security incident occurs concerning the application.

2) Application Security Plan. Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST. Advice and comment on the plan shall be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation. Application security plans shall include:

   a) Application Rules. Establish a set of rules concerning use of and behavior within the application. The rules shall be as stringent as necessary to provide adequate security for the application and the information in it. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules.

   b) Specialized Training. Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may 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).

   c) Personnel Security. Incorporate controls such as separation of duties, least privilege and individual accountability into the application and application rules as appropriate. In cases where such controls cannot adequately protect the application or information in it, screen individuals commensurate with the risk and magnitude of the harm they could cause. Such screening shall be done prior to the individuals' being authorized to access the application and periodically thereafter.

   d) Contingency Planning. Establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support.

e) Technical Controls. Ensure that appropriate security controls are specified, designed into, tested, and accepted in the application in accordance with appropriate guidance issued by NIST.

f) Information Sharing. Ensure that information shared from the application is protected appropriately, comparable to the protection provided when information is within the application.

g) Public Access Controls. Where an agency's application promotes or permits public access, additional security controls shall be added to protect the integrity of the application and the confidence the public has in the application. Such controls shall include segregating information made directly accessible to the public from official agency records.

3) Review of Application Controls. Perform an independent review or audit of the security controls in each application at least every three years. Consider identifying a deficiency pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act if there is no assignment of responsibility for security, no security plan, or no authorization to process for the application.

4) Authorize Processing. Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.

Appendix C. Material Control Weakness

OMB Circular A-123 requires agencies to test and report annually on the adequacy of organizational management controls. Agency managers and employees should report any deficiencies in management controls if the deficiency is or should be of interest to the next level of management. Agency employees and managers generally report deficiencies to the next supervisory level, which allows the chain of command structure to determine the relative importance of each deficiency.

The Circular states:

> A deficiency that the agency head determines to be significant enough to be reported outside the agency (i.e. included in the annual Integrity Act report to the President and the Congress) shall be considered a "material weakness." This designation requires a judgment by agency managers as to the relative risk and significance of deficiencies. Agencies may wish to use a different term to describe less significant deficiencies, which are reported only internally in an agency. In identifying and assessing the relative importance of deficiencies, particular attention should be paid to the views of the agency's IG.

NASA Policy Directive 1200.1A, "Internal Management Controls and Audit Liaison and Followup," dated June 1, 2000, requires managers to identify and recommend significant areas of management concern that may be the result of weak, inadequate, or unenforced management controls. Center Directors forward significant areas of concern to their Institutional Program Office Associate Administrator. The Associate Administrators report their concerns to the Administrator. Headquarters Officials in Charge submit significant areas of management concern to the Internal Control Council, which makes recommendations to the Administrator. The NASA Inspector General is an ex-officio member of the Internal Control Council and submits significant areas of concern to the Council. The Administrator decides which concerns will be reported under the Federal Managers' Financial Integrity Act.

Appendix D. Management's Response

National Aeronautics and
Space Administration
Office of the Administrator
Washington, DC 20546-0001

SEP 25 2000

TO: W/Assistant Inspector General for Auditing

FROM: AO/Chief Information Officer

SUBJECT: Draft Report on Audit of System Information Technology Security Planning, Assignment Number A0003700

Thank you for the opportunity to review and comment on the subject draft report. Management is fully aware of the need to improve IT Security and is working with each Center CIO and ITS managers to schedule and implement a number of IT security measures.

At the time this audit was conducted many of the Agency's Special Management Attention (SMA) IT system plans were not completed as stated, however, since that time much work has been done to ensure that all SMA systems have approved IT security plans, this is scheduled to be completed by September 30, 2000.

The draft report contained the following eight recommendations.

The NASA Chief Information Officer should:

1) Create an inventory of every NASA IT system and the status of the supporting IT security plans and required authorizations to process. The inventory should identify those systems for which NASA management will have separate security plans for each major element or component of the IT system.

Concur: 1. SMA systems inventory will be maintained at the Agency CIO office from data provided from the Centers. 2. Other systems inventory will be maintained at the Centers with access from CIO office.

2) Require the Centers and the Jet Propulsion Laboratory to submit quarterly status reports until there is a current security plan and authorization to process for each IT system or system element.

Concur: The CIO requires a quarterly status report on priority systems, which are determined each year. For FY2000 the priority systems are defined as SMA systems.

3) The Associate Administrator for Headquarters Operations should report to the Agency's Internal Control Council the Headquarters' Federal noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

Partially Concur: While not fully compliant with 2810.1 at the time of the audit, deficiencies have been noted and a schedule has been developed to rectify these deficiencies. All SMA systems are scheduled to have fully compliant IT Security plans with CIO approval by September 30, 2000, all HQ general support systems will have IT Security plans by April 30, 2001. With completion of these plans there is no need to report noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

4) The Associate Administrator for Space Science should report to the Agency's Internal Control Council the Jet Propulsion Laboratory Federal noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

Partially Concur: JPL plans to complete IT plans for all SMA systems by September 30, 2000. The planned completion date for IT plans on the remaining applicable JPL computer systems is by September 30, 2001. We are in agreement that the requirement for JPL to have IT security plans is necessary, this is a contract issue and not a Federal Managers' Financial Integrity Act (FMFIA) issue. Because of JPL's status as a contractor-operated installation, JPL does not participate in the Agency's internal control process. Our contractual relationship with the California Institute of Technology, which manages JPL, provides for assessments of contractor performance through the mechanism of semiannual performance evaluations.

5) The Director, John H. Glenn Research Center at Lewis Field, should report to the Associate Administrator for Aerospace Technology the Glenn Federal noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

Concur: Glenn Research Center has already reported this condition in their August 15, 2000, Federal Manager's Financial Integrity Act annual statement of assurance. GRC has a project plan in place to complete the development of IT Security Plans for all SMA systems by September 30, 2000, and the remaining IT system security plans by September 30, 2002.

The Director, Goddard Space Flight Center, should:

6) Report to the Associate Administrator for Earth Science the major IT system Federal noncompliance conditions as a significant are of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

7) Expedite the development and implementation of the required security plans, contingency plans, and risk assessments for the major IT system.

Concur: The Directors Statement of Assurance to the Associate Administrator for Earth Science highlights IT Security as one of three areas for special discussion and contained the following statement. "Finally in the area of IT security, I would like to assure you that we are addressing IT security issues surfaced by the NASA Office of Inspector General (OIG). In particular, the NASA OIG draft audit report A0003700 entitled "System Information Technology Security Planning," dated August 25, 2000, noted that NASA, along with GSFC as one of its Centers, has not adequately complied with the Computer Security Act and Office of Management and Budget (OMB) Circular A-130. The draft report noted that five of fourteen major elements of a major information system at GSFC did not have properly documented security plans, contingency plans, or risk assessments. This formalized planning and documentation deficiency can reduce the effectiveness of the implemented IT security programs for this information system. GSFC is taking steps to expedite the proper development and implementation of the required security plans, contingency plans, and risk assessments for this system.

"These steps include the completion of an internal GSFC audit to document deficiencies against OMB Circular A-130 requirements and continuation of efforts to update, or create as needed, the required plans and assessments to ensure compliance by each element. In parallel, we will continue to implement technical security controls in order to mitigate security risks. Each of the specified elements of this major information system will deliver by the end of the calendar year a comprehensive security plan, contingency plan, and risk assessment, as required by OMB A-130, to the major element IT Security Official (ITSO). The ITSO will present these plans and assessments to the GSFC CIO for his review."

8) The Director, Langley Research Center, should report to the Associate Administrator for Aerospace Technology the Langley Federal noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

Partially Concur: All of the Langley Research Center SMA system plans are scheduled to be in place by September 30, 2000. With the completion of these plans there is no need to report noncompliance conditions as a significant area of concern to be included in NASA's annual Federal Managers' Financial Integrity Act statement of assurance.

The NASA Chief Information Officer should revise NPG 2810.1 to comply with OMB circular A-130 requirements. Specifically, the NPG should be revised to require:

9) Periodic screening of individuals who are authorized to bypass significant technical and operational controls of IT systems.

Concur: Compliance with OMB Circular A-130 will be addressed in the next revision of NPG 2810.

10) Initial and periodic screening of all individuals commensurate with the risk and magnitude of the harm they could cause when applications or the information in the application are not adequately protected because controls such as individual accountability are not used or do not provide sufficient protection.

Concur: Compliance with OMB Circular A-130 will be addressed in the next revision of NPG 2810.

Lee B. Holcomb

cc:
AO/D. Nelson
AO/C. Simonson
CI/ S. Daniels-Gibson
JM/H. Robbins
GRC/S. Pillay
GSFC/M. Halem
JPL/T. Renfrow
LaRC/C. Mangum

Appendix E. Report Distribution

National Aeronautics and Space Administration (NASA) Headquarters

A/Administrator
AI/Associate Deputy Administrator
AO/Chief Information Officer
B/Chief Financial Officer
B/Comptroller
BF/Director, Financial Management Division
C/Associate Administrator for Headquarters Operations
G/General Counsel
H/Associate Administrator for Procurement
HK/Director, Contract Management Division
HS/Director, Program Operations Division
J/Associate Administrator for Management Systems
JM/Acting Director, Management Assessment Division
L/Associate Administrator for Legislative Affairs
M/Associate Administrator for Space Flight
R/Associate Administrator for Aerospace Technology
S/Associate Administrator for Space Science
Y/Associate Administrator for Earth Science

NASA Centers

Director, Ames Research Center
  Chief Information Officer, Ames Research Center
Director, John H. Glenn Research Center at Lewis Field
  Chief Information Officer, John H. Glenn Research Center at Lewis Field
Director, Goddard Space Flight Center
  Chief Information Officer, Goddard Space Flight Center
Director, Jet Propulsion Laboratory
  Chief Information Officer, Jet Propulsion Laboratory
Director, Lyndon B. Johnson Space Center
  Chief Information Officer, Lyndon B. Johnson Space Center
Director, John F. Kennedy Space Center
  Chief Information Officer, John F. Kennedy Space Center
  Chief Counsel, John F. Kennedy Space Center
Director, Langley Research Center
  Chief Information Officer, Langley Research Center
Director, George C. Marshal Space Flight Center
  Chief Information Officer, George C. Marshal Space Flight Center

Non-NASA Federal Organizations and Individuals

Assistant to the President for Science and Technology Policy
Deputy Associate Director, Energy and Science Division, Office of Management and Budget
Branch Chief, Science and Space Programs Branch, Energy and Science Division, Office of Management and Budget
Associate Director, National Security and International Affairs Division, Defense Acquisitions Issues, General Accounting Office
Professional Assistant, Senate Subcommittee on Science, Technology, and Space

Chairman and Ranking Minority Member – Congressional Committees and Subcommittees

Senate Committee on Appropriations
Senate Subcommittee on VA, HUD, and Independent Agencies
Senate Committee on Commerce, Science, and Transportation
Senate Subcommittee on Science, Technology, and Space
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on VA, HUD, and Independent Agencies
House Committee on Government Reform and Oversight
House Subcommittee on Government Management, Information, and Technology
House Subcommittee on National Security, Veterans Affairs, and International Relations
House Committee on Science
House Subcommittee on Space and Aeronautics, Committee on Science

Congressional Member

Honorable Pete Sessions, U.S. House of Representatives

NASA Assistant Inspector General for Auditing
Reader Survey

The NASA Office of Inspector General has a continuing interest in improving the usefulness of our reports. We wish to make our reports responsive to our customers' interests, consistent with our statutory responsibility. Could you help us by completing our reader survey? For your convenience, the questionnaire can be completed electronically through our homepage at http://www.hq.nasa.gov/office/oig/hq/audits.html or can be mailed to the Assistant Inspector General for Auditing; NASA Headquarters, Code W, Washington, DC 20546-0001.

Report Title: System Information Technology Security Planning

Report Number: _____ **Report Date:** _____

Circle the appropriate rating for the following statements.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	N/A
1. The report was clear, readable, and logically organized.	5	4	3	2	1	N/A
2. The report was concise and to the point.	5	4	3	2	1	N/A
3. We effectively communicated the audit objectives, scope, and methodology.	5	4	3	2	1	N/A
4. The report contained sufficient information to support the finding(s) in a balanced and objective manner.	5	4	3	2	1	N/A

Overall, how would you rate the report?

Excellent Fair
Very Good Poor
Good

If you have any additional comments or wish to elaborate on any of the above responses, please write them here. Use additional paper if necessary. _____

_____

_____

_____

_____

_____

How did you use the report? _____

_____

_____

_____

_____

_____

_____

How could we improve our report? _____

_____

_____

_____

_____

_____

_____

How would you identify yourself? (Select one)

Congressional Staff	Media
NASA Employee	Public Interest
Private Citizen	Other: _____
Government: _____ Federal: _____ State: _____ Local: _____	

May we contact you about your comments?

Yes: _____ **No: _____**

Name: _____

Telephone: _____

Major Contributors to the Report

Gregory B. Melson, Program Director, Information Assurance Audits

Ernest L. Willard, Audit Program Manager

James W. Geith, Auditor-in-Charge

Kathleen M. Kirby, Auditor

Kenneth E. Sidney, Auditor

Brenda K. Stepps, Auditor

Nancy C. Cipolla, Report Process Manager