IG-01-022

AUDIT REPORT

INFORMATION TECHNOLOGY SECURITY PLANNING

March 30, 2001

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 www.hq.nasa.gov/office/oig/hq/audits.html.

Acronyms

ASIS	American Society for Industrial Security
GAO	General Accounting Office
GPRA	Government Performance and Results Act
IT	Information Technology
NPD	NASA Policy Directive
NPG	NASA Procedures and Guidelines
OMB	Office of Management and Budget
PCIE	President's Council on Integrity and Efficiency

W March 30, 2001

TO: A/Administrator

FROM: W/Inspector General

SUBJECT: INFORMATION: Information Technology Security Planning
Report Number IG-01-022

The NASA Office of Inspector General has completed an audit of System Information Technology Security Planning. We found that NASA has established adequate processes to ensure information technology (IT) security is considered as a part of the Agency's strategic information resource program planning. NASA has established many new IT security policies in response to the General Accounting Office (GAO) report number GAO/AIMD-99-47, "Information Security, Many NASA Mission-Critical Systems Face Serious Risks," May 1999,[1] and NASA's internal "Information Technology Security Program Review," August 1998.[2] The new policies are adequate, but substantial work remains to fully implement them. However, the limited metrics in the fiscal year 2001 performance plan do not provide an adequate assessment of NASA's IT security program. [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).

]

[1] See Appendix B a summary of the GAO report and Appendix C for the open recommendations.
[2] See Appendix C for a summary of the NASA internal IT security review.

Background

On October 30, 2000, the President signed into law the fiscal year 2001 Defense Authorization Act (Public Law 106-398) including Title X, subtitle G, "Government Information Security Reform" (The Security Act). The Security Act provides a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets and a mechanism for improved oversight of Federal agency information security programs. The Government Performance and Results Act of 1993 (GPRA) requires Federal agencies to set goals, targets,[3] and indicators to gauge performance and report annually to the Congress on agency success in meeting those goals. One of NASA's targets for fiscal year 2001 is to enhance IT security through a reduction of system vulnerabilities at all NASA Centers. [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).
]

Recommendations

We recommended that the NASA Chief Information Officer include a description of the time and resources necessary to implement the Agency's information security program in NASA's annual performance plans and develop additional GPRA IT security metrics. These actions will provide the Congress with the information required by the Security Act and improve NASA's ability to measure the performance of its IT security program. We also recommended that NASA select vulnerabilities that ensure the data for the current IT systems vulnerability performance indicator accurately reflects the Agency's IT security risk. Increasing the number of vulnerabilities tested by selecting more recently discovered vulnerabilities will better measure the risk to NASA's IT systems. Finally, we recommended that NASA describe the extent of IT security vulnerability testing in the annual GPRA report. This explanation will enable the Congress to better understand the metric currently used to measure reductions in IT system vulnerability.

Management's Response

NASA concurred with three of the recommendations and partially concurred with the recommendation to select vulnerabilities that ensure the data for the current IT systems vulnerability performance indicator accurately reflects NASA's IT security risk. NASA did not fully concur due primarily to concerns about the amount of additional testing for vulnerabilities that might be required. Nonetheless, NASA has already changed the metric and requested that the Centers scan for an updated list of vulnerabilities and is planning to update the metric

[3] Target is the term NASA uses in the Performance Plan for those measures or metrics that the Agency established to accomplish (and measure) the individual goals and objectives.

periodically. In addition, the Chief Information Officer has agreed to work collaboratively with my office on the amount of testing required.

Details on the status of the recommendations are in the finding section of the report.

[original signed by]
Roberta L. Gross

Enclosure

Final Report on Audit of Information Technology
Security Planning

FINAL REPORT
INFORMATION TECHNOLOGY SECURITY PLANNING

W March 30, 2001

TO: AO/Chief Information Officer

FROM: Assistant Inspector General for Auditing

SUBJECT: Final Report on the Audit of Information Technology Security Planning
Assignment Number A0003701
Report Number IG-01-022

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 recommendations will remain open for reporting purposes until corrective action is completed. Please notify us when action has been completed on the recommendations, 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; Mr. Ernest L. Willard, Program Manager, Information Assurance Audits; at (650) 604-2676, 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 G.

[original signed by]
Russell A. Rau

Enclosure

cc:
B/Acting Chief Financial Officer
B/Comptroller
BF/Director, Financial Management Division
G/General Counsel
JM/Director, Management Assessment Division
KSC/AA/Director, John F. Kennedy Space Center

Contents

NASA Office of Inspector General

IG-01-022 **March 30, 2001**
A0003701

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 attacks. The single most important factor in prompting the establishment of an effective IT security program is 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.

Objectives. The overall audit objective was to determine whether NASA had established and implemented effective policies and procedures for IT security planning in accordance with Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," dated February 8, 1996. Specifically, we determined whether the Agency:

- established effective IT security planning processes as an integral part of its strategic information resources management program and

- developed adequate IT system vulnerability metrics for reporting under GPRA.

The originally announced audit objectives included determining whether NASA had established and implemented effective security plans for general-support systems,[4] major applications,[5] and publicly accessible Web sites.[6] We covered this objective in audit report number IG-00-055, "System Information Technology Security Planning," dated September 28, 2000, which is summarized in Appendix B.

We also reviewed management actions on the recommendations from NASA's internal "Information Technology Security Program Review," August 1998 and GAO report

---

[4] 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."

[5] 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."

[6] 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.

number GAO/AIMD-99-47, "Information Security, Many NASA Mission-Critical Systems Face Serious Risks," May 1999. Details on our objectives, scope, and methodology are in Appendix A.

Results of Audit. NASA has established adequate processes to ensure IT security is considered as a part of the Agency's strategic information resource program planning. NASA has completed corrective actions for 7 of the 11 recommendations from NASA's 1998 internal IT security review and 8 of the 9 recommendations from the GAO report that affect IT security planning. Many of these recommendations relate to implementing new policies as shown in Appendix C. Overall, the new policies that NASA established are adequate, but substantial work remains to fully implement them.

However, NASA's current policies for scanning its computer systems for a limited number of vulnerabilities do not result in an adequate assessment of the Agency's IT system vulnerabilities. Specifically, the limited metrics in the fiscal year 2001 performance plan do not provide an adequate assessment of NASA's IT security program. As a result, the IT security risks and metrics that NASA reports to the Congress may understate NASA's IT vulnerabilities and provide undue assurance on the integrity, availability, and confidentially of information.

Other Matters of Interest. [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5). [7]

[8]

]

(Appendix D).

Recommendations. We recommend that the NASA Chief Information Officer (1) include a description of the time and resources necessary to implement the Agency's information security program in the Agency annual performance plans, (2) develop additional GPRA IT security metrics, (3) select vulnerabilities that more accurately reflect NASA's IT security risk, and (4) describe the extent of IT security vulnerability testing in the GPRA report.

---

[7] The seven Centers that had designated their financial management systems as "special management attention" systems were Ames Research Center, Goddard Space Flight Center, John H. Glenn Research Center at Lewis Field, Lyndon B. Johnson Space Center, the Jet Propulsion Laboratory, Langley Research Center, and George C. Marshall Space Flight Center.

[8] "Special management attention" is a NASA term applied to information systems that require increased oversight due to the risk and magnitude of harm that would result from the loss, misuse, unauthorized access to or modification of the data in the system.

Management's Response. Management concurred with all but one recommendation. Management partially concurred with the recommendation to select vulnerabilities that more accurately reflect NASA's IT security risk. However, NASA has already changed the metric and has asked the Centers to scan for an updated list of vulnerabilities. Further, the Chief Information Officer will coordinate with the Inspector General's Office on the amount of testing for vulnerabilities.

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

Introduction

NASA Policy Directive 1000.1a, "NASA Strategic Plan 2000," defines the vision, mission, and fundamental questions of science and research that provide the foundation of the Agency's goals. The Strategic Plan describes the five Strategic Enterprises that manage the programs and activities to implement NASA's mission, answer the fundamental questions, and provide service to identified customers. The Strategic Enterprises are: Space Science, Earth Science, Biological and Physical Research, Human Exploration and Development of Space, and Aerospace Technology. The Strategic Plan also defines the Crosscutting Processes that support the Strategic Enterprises. The Crosscutting Processes are Manage Strategically, Provide Aerospace Products and Capabilities, Generate Knowledge, and Communicate Knowledge. One of the objectives of Manage Strategically is to "Enhance the security, efficiency, and support provided by our information technology resources."

To achieve security in computing, NASA Procedures and Guidelines (NPG) 2810.1, "Security of Information Technology," dated August 26, 1999, requires that NASA maintain the following three components of IT resources:

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.

Finding and Recommendations

Finding. NASA's Information System Vulnerability Metric

NASA's annual performance plan limits discussion of IT security programs to one performance target. In addition, NASA's current practices for computer system vulnerability scanning do not result in an accurate assessment of NASA's IT system vulnerabilities. [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).

]

Government Performance and Results Act

Congress enacted the GPRA to improve the efficiency of all Federal agencies. GPRA's specific goals are to:

- Improve Federal program management, effectiveness, and public accountability.
- Improve congressional decision making on where to commit the Nation’s financial and human resources.
- Improve citizen confidence in Government performance.

The GPRA directed Executive Branch agencies to develop a customer-focused strategic plan that aligns activities with concrete missions and goals. GPRA directed agencies to manage and measure results to justify congressional appropriations and authorizations. Federal agencies are required to prepare and submit an annual Performance Plan to the Director of the Office of Management and Budget and the Congress. The plan should establish objective and measurable performance goals, establish performance indicators to be used in measuring relevant outputs or other results, provide a basis for comparing actual results with the established goals, and describe the means to be used to verify and validate measured values. Six months after the end of each fiscal year, agencies report on the degree of success in achieving the goals and evaluation measures defined in the strategic and performance plans.

Government Information Security Reform

The Security Act codifies the existing requirements of OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," and requires agencies to:

- incorporate security into the life cycle of agency information systems,

- develop an agencywide information security program, and

- conduct annual reviews of their information security programs and report the results to OMB for consolidation into a report to the Congress.

The Security Act also requires each agency's Chief Information Officer to include a description of the time periods and resources that are necessary to implement the information security program in the annual performance plan required by GPRA.

NASA's Fiscal Year 2001 Performance Plan

The NASA 2001 Performance Plan does not contain a description of the time periods and resources that are necessary to implement the information security program as required by the Security Act because NASA issued the plan before the Security Act became law. Nevertheless, such information provides basic parameters contemplated under GPRA[9] and thus should be reported in the Performance Plan.

NASA's coverage of its IT security program in the fiscal year 2001 Performance Plan is limited to a target to improve IT infrastructure and enhance IT security as follows:

> Target**:** Improve IT infrastructure service delivery to provide increased capability and efficiency while maintaining a customer rating of "satisfactory," and **enhance IT security through a reduction of system vulnerabilities across all NASA centers**, [emphasis added] emphasizing IT security awareness training for all NASA personnel.[10]

To measure the reduction of system vulnerabilities, NASA chose a performance indicator that uses the results of IT system vulnerability scans. However, this indicator measures NASA's vulnerabilities to only a limited number of threats. The indicator does not provide a complete picture of NASA's IT security programs.

System Vulnerabilities

The National Institute of Standards and Technology issued a handbook, "An Introduction to Computer Security," Special Publication 800-12, to provide guidance to computer security personnel.[11] The handbook states:

---

[9] OMB requires an agency to briefly describe the operational processes, skills, and technology and the human, capital, information, or other resources required to meet the performance goals.

[10] NASA Inspector General Report G-00-019, "Assessment of Information Technology Security Training and Development and Other Human Resource Considerations, " February 6, 2001, discusses a review of NASA's IT security awareness and training metrics.

[11] In the Computer Security Act of 1987, the Congress assigned the responsibility to prepare standards and guidelines for the security of sensitive Federal systems to the National Institute of Standards and Technology.

> Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet" to avoid unfavorable publicity. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system. . . .
>
> To control the risks of operating an information system, managers and users need to know the vulnerabilities of the system and the threats that may exploit them. Knowledge of the threat environment allows the system manager to implement the most cost-effective security measures. In some cases, managers may find it more cost-effective to simply tolerate the expected losses. Such decisions should be based on the results of a risk analysis.

Common threats include:

- errors and omissions by data entry clerks and system users;
- computer fraud and theft by insiders or outsiders;
- employee sabotage;
- loss of physical and infrastructure support;
- hackers;
- industrial, economic, and foreign government espionage;
- malicious code such as viruses, worms,[12] and Trojan horses;[13] and
- threats to personal privacy.

See Appendix E for an extract of the handbook's Chapter 4, "Common Threats: A Brief Overview."

[12] A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.
[13] A Trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves.

NASA's Quarterly Vulnerability Scans

To demonstrate that NASA is enhancing IT security through the reduction of system vulnerabilities, NASA is scanning its computer systems[14] quarterly [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).] and collecting the data for its FY 2001 Performance Report, which is due March 31, 2002. Each NASA Center performs the quarterly scans and reports the data to the Principal Center for IT Security at Ames Research Center (Ames). The Principal Center for IT Security accumulates the data and presents it to the Congress in an annual performance report.

NASA managers use the scanning results to make improvements to their IT systems. After the Center performs the quarterly scans, NASA managers take actions to correct the vulnerabilities. Subsequently, the managers can ask for a rescan of their IT systems to determine whether they were successful in fixing the problem. This ongoing process results in a continual improvement of the security of the IT systems, particularly for the [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).]

Scanning Software Limitations

NASA does not use scanning software to detect many types of vulnerabilities. NASA's Principal Center for IT Security, in conjunction with the Centers Chief Information Officers, decided to use the a software package[15] that NASA owned when it started to scan computer systems. The [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).] software performs scheduled or event-driven probes of network communication services, operating systems, routers, e-mail and Web servers, firewalls, and applications, thereby identifying system weaknesses that could be exploited by intruders to gain access to the network. Hackers and persons conducting industrial, economic, and foreign government espionage often exploit these vulnerabilities. [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).
]

[Paragraph withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).

16

[14] [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).

]

[15] [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).

]

[16] UNIX is an immensely powerful and complex operating system that provides multitasking and multiuser capabilities on a single computer.

]

NASA Uses Only Part of the [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).] **Software Capabilities**

NASA's Information Technology Security Manager, in conjunction with the Center Chief Information Officers, decided to use an [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).] software package[17] as a tool for gathering metric information for GPRA reporting. [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).
[18]] The Agency established the baseline because of concern that too much time would be expended checking for nonexistent problems as a result of vulnerability tests that report the existence of a vulnerability when none exists. [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).
.[19]]

However, the [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).] software provides more capability than NASA utilizes. As of November 30, 2000, the [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).] software database contained tests for 802 vulnerabilities, and the capability to write custom code to scan for vulnerabilities that the software does not address in its current database. Further, [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).] has grouped its 802 vulnerabilities into 38 categories that represent various types of vulnerabilities. [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).]

New Vulnerabilities Are Discovered Daily

Hackers constantly find new ways to exploit systems. Therefore, [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).] continually updates its database to include additional vulnerability checks for newly identified exploits of networks and data. For example, from August 2000 through December 2000, [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).] issued 5 updates to its software that added 75 additional vulnerability checks. [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).] considers 40 of those 75 new vulnerabilities to be high risk. [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).]

Annual Security Act Reviews

The Security Act requires that Agency program officials, in consultation with the Chief Information Officer, review each Agencywide information security program at least annually.

---

[17] [Withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).]

[18] In addition to the quarterly scans for the annual performance report, each Center may scan for any vulnerabilities it chooses for its internal purposes; some Centers are doing this.

[19] At the time we performed the field work on vulnerability scanning (August to November 2000), NASA was still developing its scanning procedures and learning how to use the software. We did not test the scanning data after NASA revised its procedures.

The annual review should include reviews of all programs included in the Agencywide program. To promote consistent reviews across the Government, the Chief Information Officer Council had the National Institute of Standards and Technology prepare the "Federal Information Technology Security Assessment Framework," dated November 28, 2000. Agencies can use the Framework coupled with the National Institute of Standards and Technology Self-Assessment Questionnaire[20] to assess the status of security controls for individual systems (that is, general-support systems, major applications, mission-critical systems) or a logically related group of systems that support operational programs.

Conclusion

NASA will report data to the Congress that could understate NASA's actual vulnerability to misuse, theft, or destruction of Government IT resources and provide undue assurance on the effectiveness of NASA's IT security program. We believe that the Congress' intent for GPRA and the annual performance reporting requirement is that the annual reports adequately and accurately state the results of any metrics used to measure performance against established targets and goals in the annual performance plans. Therefore, NASA should revise the current metric to reflect a more appropriate scan of significant and current vulnerability checks and make clear to the Congress that a specific, limited set of vulnerabilities are being reported. NASA should also indicate to the Congress how the Agency determined the appropriateness of the metrics. NASA should add information to the annual performance plan to show the time and resources required to implement its Agencywide IT security program.

The Security Act requirement to include information on the Agency's information security program in the annual performance plan and the requirement to submit an annual evaluation on the Agency's information security program indicate that the Congress wants comprehensive information on the Agency's IT security program. Therefore, NASA should expand coverage of the Agency's information security program in the annual performance plan.

Recommendations, Management's Response, and Evaluation of Response

The NASA Chief Information Officer should:

1. **Include in the Agency annual performance plans a description of the time and resources that are necessary to implement the Agency's information security program as contemplated by GPRA and as required by the Government Information Security Reform, starting with the fiscal year 2003 plan. Also include in the annual performance plan the metrics for measuring the implementation of the Agency's information security program.**

[20] The National Institute of Standards and Technology will issue the Self-Assessment Questionnaire in 2001 as a National Institute of Standards and Technology Special Publication.

Management's Response. Concur. The Chief Information Officer already has a requirement in the IT portion of the NASA FY 2003 Program Operating Plan Call for Centers to identify the resources needed to implement the Agency's IT Security Program. The Chief Information Officer will seek to modify the FY 2003 annual performance plan to include the schedule and requirements mandated by the Government Information Security Reform Act. The Chief Information Officer will include metrics for implementation of the IT security plan and will baseline those requirements in FY 2002. The complete text of management's response is in Appendix F.

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.

2. Develop additional GPRA IT security metrics to cover the requirements of OMB Circular A-130, Appendix III.

Management's Response. Concur. NASA already gathers metrics on the four requirements of OMB Circular A-130, Appendix III, which address assigned responsibility, security plans, authorization to process, and periodic review. The Chief Information Officer will seek to add an additional IT Security GPRA metric, beginning in 2003, that will track the review of security controls for "special management attention"[21] systems (see Appendix F).

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.

3. Select vulnerabilities that ensure the data for the current IT systems vulnerability performance indicator accurately reflects NASA's IT security risk.

Management's Response. Partially concur. NASA agrees with our intent that the Chief Information Officer modify the metric to better reflect current vulnerabilities. When the metric was established in 1999, scanning tools were less mature than they are today. With the benefit of experience, NASA has already requested that the Centers change the metric to scan for an updated list of vulnerabilities and is planning to update the metric periodically. NASA is concerned about our use of the word "ensure." Exhaustive testing for every vulnerability is not cost-effective and yields false positives. It is not currently possible to "ensure" that the performance indicator accurately reflects NASA's IT security risk. NASA believes that the current vulnerability testing reflects a balance of effectiveness and cost; however, the Chief Information Officer will work collaboratively with the Inspector General's office to retain proper balance between effective and exhaustive vulnerability testing (see Appendix F).

[21] See footnote 8.

Evaluation of Management's Response. Management's proposed actions are responsive to the intent of the recommendation. We did not intend to imply that exhaustive testing for every possible vulnerability was necessary. We were concerned that the list of vulnerabilities had become outdated and should be revised to include new vulnerabilities that hackers are using to attack NASA computer systems. The recommendation is resolved but will remain undispositioned and open until agreed-to corrective actions are completed.

4. Describe the extent of vulnerability testing used to calculate the IT security metric in NASA's annual performance report to Congress.

Management's Response. Concur. The FY 2002 Performance Plan has been modified to more clearly state that only a specified set of vulnerabilities is included in the metric and that the scanned vulnerabilities may change from quarter to quarter (see Appendix F).

Evaluation of Management's Response. Management's proposed actions are responsive to the intent of the recommendation. The recommendation is resolved but will remain undispositioned and open until we are able to review the FY 2002 Performance Plan and the FY 2001 report to Congress.

Appendix A. Objectives, Scope, and Methodology

Objectives

The overall objective was to determine whether NASA has established and implemented effective policies and procedures for information technology (IT) security planning in accordance with Office of Management and Budget (OMB) Circular A-130. [22] Specifically, we determined whether the Agency has:

- established effective IT security planning processes as an integral part of its strategic information resources management program and

- developed adequate IT system vulnerability metrics for reporting under the Government Performance and Results Act (GPRA).

The originally announced audit objectives included determining whether NASA had established and implemented effective security plans for general-support systems, major applications, and publicly accessible Web sites. We covered this objective in audit report number IG-00-055, "System Information Technology Security Planning," September 28, 2000. The report is summarized in Appendix B.

We also reviewed the actions NASA management has taken on the recommendations from NASA's internal "Information Technology Security Program Review," and the General Accounting Office (GAO) report number GAO/AIMD-99-47, "Information Security, Many NASA Mission-Critical Systems Face Serious Risks." A summary of NASA's internal review is in Appendix C. A summary of the GAO report is in Appendix B.

Scope and Methodology

We performed work at NASA Headquarters, Ames Research Center (Ames), Goddard Space Flight Center (Goddard), John H. Glenn Research Center at Lewis Field (Glenn), Lyndon B. Johnson Space Center (Johnson), John F. Kennedy Space Center (Kennedy), the Jet Propulsion Laboratory (JPL), Langley Research Center (Langley), and George C. Marshall Space Flight Center (Marshall). We reviewed NASA and Center directives, documents, plans, and reports related to the implementation of Federal laws and regulations and NASA policies on IT security, information resource management, strategic planning, and measuring performance. We interviewed NASA and contractor

[22] 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.

personnel on IT security planning. We also reviewed the management actions taken in response to the GAO report on NASA's IT security and NASA's internal IT security review.

We also interviewed NASA and contractor personnel on the development of the GPRA metric for reducing IT system vulnerabilities across all NASA Centers. We examined the capability of the quarterly scans to identify different types of vulnerabilities. We reviewed a sample of the quarterly IT system scan results at Johnson, Marshall, and Goddard by testing the procedures that NASA has developed for collecting information that the Agency will use to report whether it has met its goal of reducing IT system vulnerabilities.

Management Controls Reviewed

We reviewed NASA policies and procedures on strategic planning to determine whether IT security was included in the process. We also reviewed management controls relative to the fiscal year 2001 Performance Plan target for reducing IT system vulnerability. We reviewed the procedures for conducting the quarterly scans and reporting the results to the Principal Center for IT Security for consolidation and incorporation into the annual performance report for fiscal year 2001.

We determined that controls needed to be strengthened to ensure that vulnerability scanning of NASA's IT systems is appropriate as discussed in the Finding section of the report.

Audit Field Work

We performed field work from August 2000 through January 2001 at NASA Headquarters, Ames, Goddard, Glenn, Johnson, the Jet Propulsion Laboratory, Kennedy, Langley, and Marshall. We performed the audit in accordance with generally accepted government auditing standards.

Appendix B. Summary of Prior Audit Coverage

The NASA Office of Inspector General and the General Accounting Office (GAO) issued reports relating to information technology (IT) security planning. The reports are summarized below. (See www.hq.nasa.gov/office/oig/hq/issuedaudits.html for copies of the NASA OIG reports.)

NASA Office of Inspector General

"System Information Technology Security Planning," Report Number, IG-00-055, September 28, 2000. NASA had not adequately complied with the Computer Security Act of 1987 and Office of Management and Budget (OMB) Circular A-130. Specifically, NASA managers did not assign sufficient priority to IT security. NASA Headquarters and the Centers had no IT security plans for 17 of 38 "special management attention" systems and for 13 of 30 publicly accessible Web site host computers in our samples. The Jet Propulsion Laboratory had no IT security plans for its IT systems. In addition, there were no security plans, contingency plans, or risk assessments for five elements of a major information system. Initial and periodic personnel screening requirements in Agency policy did not comply with OMB Circular A-130 requirements. Therefore, NASA's IT systems were at increased risk, and the effectiveness of NASA's IT security program was degraded. We recommended that:

- the NASA Chief Information Officer create an inventory containing the status of IT security plans and authorizations to use the systems.

- the Centers and the Jet Propulsion Laboratory submit quarterly status reports to the NASA Chief Information Officer until there is a current security plan and authorization to process for each IT system or system element.

- the Associate Administrator for Headquarters Operations, Associate Administrator for Space Science, Director, John H. Glenn Research Center at Lewis Field, Director, Goddard Space Flight Center, and Director, Langley Research Center report the Federal noncompliance conditions to the Agency's Internal Control Council[23] as significant areas of concern.

- the Director, Goddard Space Flight Center expedite the development and implementation of IT security plans for one of NASA's major IT systems.

- the NASA Chief Information Officer expand policy requirements for personnel screenings to comply with OMB Circular A-130.

[23] 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.

NASA management fully concurred with 7 of the 10 recommendations and has completed action on 3 of them. The Centers and the Jet Propulsion Laboratory are submitting quarterly status reports on the status of their IT security plans to the NASA Chief Information Officer. The Director, Glenn Research Center at Lewis Field and the Director, Goddard Space Flight Center reported their respective Center's Federal noncompliance conditions as a significant area of concern.

NASA management partially concurred with three recommendations that the Associate Administrator for Headquarters Operations, Associate Administrator for Space Science, and the Director, Langley Research Center report the Federal noncompliance conditions to the Agency's Internal Control Council as significant areas of concern. We determined NASA management was not fully responsive to these recommendations and asked NASA management to reconsider its position.

General Accounting Office

"Information Security, Many NASA Mission-Critical Systems Face Serious Risks," Report Number GAO/AIMD-99-47, May 1999. 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, the GAO reported that 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.

Appendix B

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.

NASA management concurred with all of the GAO recommendations. See Appendix C for a summary of NASA's corrective actions.

Appendix C. Information Technology Security Recommendations

We also reviewed the actions NASA management has taken on the recommendations from NASA's 1998 internal "Information Technology Security Program Review" and the General Accounting Office (GAO) report number GAO/AIMD-99-47, "Information Security, Many NASA Mission-Critical Systems Face Serious Risks."

NASA's 1998 Internal Information Technology Security Program Review

In May 1998, the NASA Acting Deputy Administrator commissioned a special top-to-bottom review of NASA's information technology (IT) security program to determine whether NASA has the appropriate organization, policies, technologies, authorities, skills, training, and awareness to provide appropriate levels of security to assure mission performance. The review team made 33 recommendations. The recommendations included changing NASA's organization and policies, ensuring IT security plans are developed and executed, establishing IT security and risk management training programs, certifying system and network administrators, and improving incident response reporting. Eleven of the recommendations pertained to IT security planning. According to NASA management, the Agency has completed corrective action on 7 of the 11 recommendations. Table C-1 contains the four open recommendations and the status of each recommendation.

Table C-1. Open Recommendations

Recommendation	Status
The Chief Information Officer, Principal Centers,[24] and Expert Centers[25] should review and clarify their roles, responsibilities, and commitments for their assigned IT security missions. The Chief Information Officer, the appropriate Institutional Program Offices, and Center Directors should document their roles, responsibilities, and commitments to ensure that the Centers can accomplish their assignments.	Corrective actions included issuing NASA Policy Directive (NPD) 2810.1, "Security of Information Technology," on October 1, 1998, and NASA Policy and Guidelines (NPG) 2810.1 (same title as the NPD). Some of the Principal Centers and Expert Centers have established Memorandums of Understanding. The remaining actions are to complete two Memoranda of Understanding between Principal Centers and Expert Centers. Although the Memorandums of Understanding are not completed, management stated that the Expert Centers are performing their required tasks.

[24] The NASA Chief Information Officer established Principal Centers to lead or oversee projects and initiatives in specialized IT areas.

[25] Expert Centers represent exceptional Agency capabilities in certain areas of science, engineering, or technology.

Table C-1. Open Recommendations (Cont.)

Recommendation	Status
Revise NPG 7120.5A, " NASA Program and Project Management Processes and Requirements," dated April 3, 1998, to include requirements that program and project managers include security planning in the basic design of new programs. This must include risk management and assessments, security plans for IT systems processing classified and sensitive information and security for command and control communications. The revision should include identification of classified or sensitive information in any form and awareness and training measures to be taken for each program.	The Chief Information Officer and the Associate Administrator have identified the changes that will be included in the next release of NPG 7120.5A. The Office of the Chief Engineer is revising the entire NPG.
The Associate Administrator for Management Systems and Facilities and the Chief Information Officer should review all current NASA directives pertaining to IT security to ensure that all necessary facets of IT security are covered and that there are crisply defined responsibilities in each case. These responsibilities should also define and assign responsibility for NASA's external interfaces with law enforcement agencies in the case of preliminary criminal investigation.	Changes have been made to many of the more important directives, such as NPD 2810.1, "Security of Information Technology"; and NPG 1620.1, " Security Procedures and Guidelines." Other NASA directives are being reviewed during the normal review cycle.
The Office of the Chief Engineer should modify NPG 7120.5A to incorporate a requirement for security risk management throughout the life cycle of every NASA program and project, that specifically addresses and documents IT security, the security of classified information, and the protection of command, control, and communications.	The Chief Information Officer and the Associate Administrator for Security Management and Safeguards have completed identifying the additional changes that will be included in the next release of NPG 7120.5A. The Office of the Chief Engineer is revising the entire NPG.

GAO Report

GAO Report Number GAO/AIMD-99-47, "Information Security, Many NASA Mission-Critical Systems Face Serious Risks," May 1999, contained 12 recommendations. Nine of the recommendations affected IT security planning. NASA has completed action on eight of the nine recommendations. The remaining recommendation is to develop and issue guidance that specifies what information is appropriate for posting on public World Wide Web sites and that distinguishes this information from information that is sensitive and should be more closely controlled. The NASA Chief Information Officer has prepared draft guidance that the NASA Office of General Counsel is reviewing.

Appendix D. Other Matters of Interest

Federal Policies on Financial Management Systems

Office of Management and Budget (OMB) Circular A-127, "Financial Management Systems," requires that financial management systems be in place to process and record financial events effectively and efficiently and to provide complete, timely, reliable, and consistent information for decision makers and the public. This financial management information enables agencies to carry out their fiduciary responsibilities; deter fraud, waste, and abuse of Federal Government resources; and facilitate efficient and effective delivery of programs through relating financial consequences to program performance.

OMB Circular A-130, " Management of Federal Information Resources," Paragraph 8.a.1. states that agencies shall:

> (i) Consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented;
>
> (j) Record, preserve, and make accessible sufficient information to ensure the management and accountability of agency programs, and to protect the legal and financial rights of the Federal Government.

The Joint Financial Management Improvement Program directive, "Framework for Federal Financial Management Systems," January 1995, states:

> Computer systems, databases, and communication networks are key components of the information technology infrastructure upon which financial management systems depend. Computer security is an important element of internal control; it is essential for the operations of systems and the accuracy of the financial data collected, stored, and reported.

NASA Information Technology Security Policy

NASA Procedures and Guidelines (NPG) 2810.1, "Security of Information Technology," requires that the Center Chief Information Officers, Center Information Technology (IT) Security Managers, Organization Computer Security Officials, and line managers identify any systems that require "special management attention."[26] Once systems are identified as requiring "special management attention," the NPG requires that senior NASA managers take a more active role in the systems' IT security programs.

[26] "Special management attention" is a NASA term applied to information systems that require increased oversight due to the risk and magnitude of harm that would result from the loss, misuse, unauthorized access to or modification of the data in the system.

The NPG also describes some specific systems that require "special management attention." These systems include:

- Major Applications - Those applications that require special attention due to the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of the information in the application.

- Major Information Systems - Systems that the NASA Chief Information Officer has designated as "major information systems" for reporting in accordance with OMB Circular A-11, "Preparing and Submitting Budget Estimates," July 19, 2000.

- Mission-Critical Systems - Systems that provide Agencywide support, such as wide area networks, Agencywide business functions, command and control of space systems, Agencywide consolidated IT resources, or IT resources that affect life support.

- NASA Resource Protection Facility - IT resources critical to a facility or operation designated under the NASA Resource Protection program by the cognizant program office.

- Center-Designated Systems - Other IT systems designated by the Center Director or Center Chief Information Officer.

[Paragraph withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).

]

[Paragraph withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).

]

Appendix D

[Paragraphs withheld per FOIA exemptions 2 & 5, 5 U.S.C. §552 (b)(2) & (5).

]

Appendix E. Common Threats

The National Institute of Standards and Technology issued the handbook, "An Introduction to Computer Security," Special Publication 800-12, to provide guidance to computer security personnel. Chapter 4 of the Handbook "Common Threats: A Brief Overview," describes some of the most prevalent threats:

> Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet" to avoid unfavorable publicity. The effects of various threats varies considerably: some affect the confidentiality or integrity of data while others affect the availability of a system.
>
> This chapter presents a broad view of the risky environment in which systems operate today. The threats and associated losses presented in this chapter were selected based on their prevalence and significance in the current computing environment and their expected growth. This list is not exhaustive, and some threats may combine elements from more than one area. This overview of many of today's common threats may prove useful to organizations studying their own threat environments; however, the perspective of this chapter is very broad. Thus, threats against particular systems could be quite different from those discussed here.
>
> To control the risks of operating an information system, managers and users need to know the vulnerabilities of the system and the threats that may exploit them. Knowledge of the threat environment allows the system manager to implement the most cost-effective security measures. In some cases, managers may find it more cost-effective to simply tolerate the expected losses. Such decisions should be based on the results of a risk analysis. . . .
>
> **4.1 Errors and Omissions**
>
> Errors and omissions are an important threat to data and system integrity. These errors are caused not only by data entry clerks processing hundreds of transactions per day, but also by all types of users who create and edit data. Many programs, especially those designed by users for personal computers, lack quality control measures. However, even the most sophisticated programs cannot

detect all types of input errors or omissions. A sound awareness and training program can help an organization reduce the number and severity of errors and omissions.

. . . Errors can occur during all phases of the systems life cycle. A long-term survey of computer-related economic losses conducted by Robert Courtney, a computer security consultant and former member of the Computer System Security and Privacy Advisory Board, found that 65 percent of losses to organizations were the result of errors and omissions. This figure was relatively consistent between both private and public sector organizations.

Programming and development errors, often called "bugs," can range in severity from benign to catastrophic. In a 1989 study for the House Committee on Science, Space and Technology, entitled *Bugs in the Program,* the staff of the Subcommittee on Investigations and Oversight summarized the scope and severity of this problem in terms of government systems as follows:

> As expenditures grow, so do concerns about the reliability, cost and accuracy of ever-larger and more complex software systems. These concerns are heightened as computers perform more critical tasks, where mistakes can cause financial turmoil, accidents, or in extreme cases, death.

Since the study's publication, the software industry has changed considerably, with measurable improvements in software quality. Yet software "horror stories" still abound . . . .

Installation and maintenance errors are another source of security problems. For example, an audit by the President's Council for Integrity and Efficiency (PCIE) in 1988 found that every one of the ten mainframe computer sites studied had installation and maintenance errors that introduced significant security vulnerabilities.

4.2 Fraud and Theft

Computer systems can be exploited for both fraud and theft both by "automating" traditional methods of fraud and by using new methods. For example, individuals may use a computer to skim small amounts of money from a large number of financial accounts, assuming that small discrepancies may not be investigated. Financial systems are not the only ones at risk. Systems that control access to any resource are targets (e.g., time and attendance systems, inventory systems, school grading systems, and long-distance telephone systems).

Computer fraud and theft can be committed by insiders or outsiders. Insiders (i.e., authorized users of a system) are responsible for the majority of fraud. A 1993 *InformationWee*k/Ernst and Young study found that 90 percent of Chief Information Officers viewed employees "who do not need to know" information as threats. The U.S. Department of Justice's Computer Crime Unit contends that "insiders constitute the greatest threat to computer systems." . . .

4.3 Employee Sabotage

Employees are most familiar with their employer's computers and applications, including knowing what actions might cause the most damage, mischief, or sabotage. The downsizing of organizations in both the public and private sectors has created a group of individuals with organizational knowledge, who may retain potential system access (e.g., if system accounts are not deleted in a timely manner). The number of incidents of employee sabotage is believed to be much smaller than the instances of theft, but the cost of such incidents can be quite high. . . .

4.4 Loss of Physical and Infrastructure Support

The loss of supporting infrastructure includes power failures (outages, spikes, and brownouts), loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, and strikes. These losses include such dramatic events as the explosion at the World Trade Center and the Chicago tunnel flood, as well as more common events, such as broken water pipes. Many of these issues are covered in Chapter 15. A loss of infrastructure often results in system downtime, sometimes in unexpected ways. For example, employees may not be able to get to work during a winter storm, although the computer system may be functional.

4.5 Malicious Hackers

The term *malicious hacker*s, sometimes called *cracker*s, refers to those who break into computers without authorization. They can include both outsiders and insiders. Much of the rise of hacker activity is often attributed to increases in connectivity in both government and industry. One 1992 study of a particular Internet site (i.e., one computer system) found that hackers attempted to break in at least once every other day.

The hacker threat should be considered in terms of past and potential future damage. Although current losses due to hacker attacks are significantly smaller than losses due to insider theft and sabotage, the hacker problem is widespread and serious. . . .

Appendix E

4.6 Industrial Espionage

Industrial espionage is the act of gathering proprietary data from private companies or the government for the purpose of aiding another company(ies). Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries. Foreign industrial espionage carried out by a government is often referred to as economic espionage. Since information is processed and stored on computer systems, computer security can help protect against such threats; it can do little, however, to reduce the threat of authorized employees selling that information.

Industrial espionage is on the rise. A 1992 study sponsored by the American Society for Industrial Security (ASIS) found that proprietary business information theft had increased 260 percent since 1985. The data indicated 30 percent of the reported losses in 1991 and 1992 had foreign involvement. The study also found that 58 percent of thefts were perpetrated by current or former employees. . . .

Within the area of economic espionage, the Central Intelligence Agency has stated that the main objective is obtaining information related to technology, but that information on U.S. Government policy deliberations concerning foreign affairs and information on commodities, interest rates, and other economic factors is also a target. The Federal Bureau of Investigation concurs that technology-related information is the main target, but also lists corporate proprietary information, such as negotiating positions and other contracting data, as a target.

4.7 Malicious Code

Malicious code refers to viruses, worms, Trojan horses, logic bombs, and other "uninvited" software. Sometimes mistakenly associated only with personal computers, malicious code can attack other platforms.

A 1993 study of viruses found that while the number of known viruses is increasing exponentially, the number of virus incidents is not. The study concluded that viruses are becoming more prevalent, but only "gradually." . . .

4.8 Foreign Government Espionage

In some instances, threats posed by foreign government intelligence services may be present. In addition to possible economic espionage, foreign intelligence services may target unclassified systems to further their intelligence missions. Some unclassified information that may be of interest includes travel plans of senior officials, civil defense and emergency preparedness, manufacturing technologies, satellite data,

personnel and payroll data, and law enforcement, investigative, and security files. Guidance should be sought from the cognizant security office regarding such threats.

4.9 Threats to Personal Privacy

The accumulation of vast amounts of electronic information about individuals by governments, credit bureaus, and private companies, combined with the ability of computers to monitor, process, and aggregate large amounts of information about individuals have created a threat to individual privacy. The possibility that all of this information and technology may be able to be linked together has arisen as a specter of the modern information age. This is often referred to as "Big Brother." To guard against such intrusion, Congress has enacted legislation, over the years, such as the Privacy Act of 1974 and the Computer Matching and Privacy Protection Act of 1988, which defines the boundaries of the legitimate uses of personal information collected by the government.

The threat to personal privacy arises from many sources. In several cases federal and state employees have sold personal information to private investigators or other "information brokers."

Appendix F. Management's Response

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

MAR 27 2001

TO: W/Assistant Inspector General for Auditing

FROM: AO/Chief Information Officer

SUBJECT: Draft Audit Report Information Technology Security Planning, Assignment Number A0003701

Thank you for the opportunity to respond to the draft report. NASA management agrees with the audit conclusion that "NASA has established adequate processes to ensure IT security is considered as a part of the Agency's strategic information resource program planning." We also agree that "Overall, the new policies that NASA established are adequate, but substantial work remains to fully implement them." NASA has strengthened its IT security program during the past 2 years and will continue to strengthen the program in coming years.

NASA management responses to the specific recommendations of the audit follow:

Recommendation 1:
The NASA Chief Information Officer should include in the Agency annual performance plans a description of the time periods and resources that are necessary to implement the Agency's information security program as contemplated by GPRA and as required by the Government Information Security Reform, starting with the fiscal year 2003 plan. Also include in the annual performance plan the metrics for measuring the implementation of the Agency's information security program.

Management response:
Concur. The CIO already has a requirement in the IT portion of the NASA FY 2003 POP Call for Centers to identify the resources needed to implement the Agency's IT Security Program. Top-level Agency IT security implementation schedules are provided on a quarterly basis by the Principal Center for IT Security lead center. We will seek to modify the FY 2003 annual performance plan to include schedule and requirements as mandated by GISRA. We will include metrics for implementation of the IT security plan and will baseline those metrics in FY 2002.

Recommendation 2:
The NASA Chief Information Officer should develop additional GPRA IT security metrics to cover the requirements of OMB Circular A-130, Appendix III.

Management response:
Concur. NASA already gathers metrics on all of the four requirements of OMB Circular A-130, Appendix III, which address assigned responsibility, security plan, authorization to process, and periodic review. We will seek to add an additional IT Security GPRA metric, beginning in 2003, which will track the review of security controls for Special Management Attention (SMA) systems.

Recommendation 3:
The NASA Chief Information Officer should select vulnerabilities that ensure the data for the current IT systems vulnerability performance indicator accurately reflects NASA's IT security risk.

Management response:
Partially concur. NASA agrees with the recommendation's intent: that we modify the metric to better reflect current vulnerabilities. When the metric was developed in 1999, scanning tools were less mature than they are today. Our reason for establishing the metric was to gain experience using a constant list of vulnerabilities as a baseline. With the benefit of that experience, NASA management has already requested that Centers change the metric to scan for an updated list of vulnerabilities, and we are planning to continue updating the metric periodically. The advantage of this approach is that, at least qualitatively, the metric will better reflect vulnerabilities as reported. The disadvantage is that what we measure will be inconsistent over time, making comparisons less meaningful.

Our area of concern with this recommendation is with the use of the word "ensure." In the audit report this recommendation is linked to a discussion of computer software that scans for vulnerabilities. Although it is state of the art, this software is immature. Exhaustive testing for every possible vulnerability is not cost effective and yields false positives. At the present time it is not possible to "ensure" that the performance indicator accurately reflects NASA's IT security risk, and we have not claimed that the metric does this. We believe that our current vulnerability testing reflects a balance of effectiveness and cost; however, we will work collaboratively with the Inspector General's office to retain proper balance between effective and exhaustive vulnerability testing.

Recommendation 4:
The NASA Chief Information Officer should describe the extent of vulnerability testing used to calculate the IT security metric in NASA's annual performance report to Congress.

Appendix F

Management response:
Concur. The FY 2002 Performance Plan has been modified to more clearly state that only a specified set of vulnerabilities are included in the metric and that the scanned vulnerabilities may change from quarter to quarter.

Lee B. Holcomb

cc:
AO/D. Nelson
AO/N. Kaplan
AO/W. Kit
JM/M. Team
W/J. Geith

Appendix G. Report Distribution

National Aeronautics and Space Administration (NASA) Headquarters

A/Administrator
AA/Chief of Staff
AI/Associate Deputy Administrator
AO/Chief Information Officer
B/Acting Chief Financial Officer
B/Comptroller
BF/Director, Financial Management Division
C/Associate Administrator for Headquarters Operations
G/General Counsel
J/Associate Administrator for Management Systems
JM/Director, Management Assessment Division
L/Acting Associate Administrator for Legislative Affairs
Z/Acting Associate Administrator for Policy and Plans

NASA Centers

Director, Ames Research Center
  Chief Information Officer, Ames Research Center
Director, Dryden Flight Research Center
  Chief Information Officer, Dryden Flight 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
Acting 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
Acting Director, John C. Stennis Space Center
  Chief Information Officer, John C. Stennis Space Center

Appendix G

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
Director, Acquisition and Sourcing Management Team, General Accounting Office
Professional Staff Member, 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 Efficiency, Financial Management, and Intergovernmental Relations
House Subcommittee on National Security, Veterans Affairs, and International Relations
House Subcommittee on Technology and Procurement Policy
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

Dennis A. Clay, Auditor

Kathy Kirby, Auditor

Patricia C. Reid, Program Assistant

Nancy C. Cipolla, Report Process Manager