United States General Accounting Office

GAO

Report to the Committee on Governmental Affairs, U.S. Senate

May 1999

INFORMATION SECURITY

Many NASA Mission-Critical Systems Face Serious Risks

GAO/AIMD-99-47

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-277744

May 20, 1999

The Honorable Fred Thompson
Chairman
The Honorable Joseph I. Lieberman
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

The National Aeronautics and Space Administration (NASA) relies on automated information systems to support a wide range of important and costly operations. In fiscal year 1998 NASA estimated that it spent $1.7 billion on information systems, including those critical to such activities as human space flight, scientific and technological development, and matters of international cooperation for the advancement of science.

Given the importance of information technology (IT) to our nation's space program, you asked us to assess NASA's information security program. Our specific objectives were to determine (1) whether NASA's mission-critical information systems [1] are vulnerable to unauthorized access, (2) whether NASA is effectively managing information systems security, and (3) what NASA is doing to address the risk of unauthorized access to mission-critical systems.

Results in Brief

Tests we conducted at one of NASA's 10 field centers showed that some of NASA's mission-critical systems at that center are vulnerable to unauthorized access. Although some of the systems we targeted had effective security mechanisms that prevented us from gaining access, we successfully penetrated several mission-critical systems, including one responsible for calculating detailed positioning data for earth orbiting spacecraft and another that processes and distributes the scientific data received from these spacecraft. Having obtained access to these systems, we could have disrupted NASA's ongoing command and control operations and stolen, modified, or destroyed system software and data.

[1] Mission-critical information systems include all systems that NASA designates as critical to fulfilling its mission, including certain administrative systems and other systems not directly supporting aerospace activities. For this review, we assessed only those mission-critical systems involved in (1) the development and operation of spacecraft, (2) the processing of scientific data, and (3) the development of aeronautics and space transportation technologies.

A major contributing factor to our ability to penetrate these systems is that NASA was not effectively and consistently managing IT security throughout the agency . We found that NASA's program did not include key elements of a comprehensive IT security management program as outlined in our May 1998 Executive Guide .[2] 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 agencywide 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 (NASIRC).

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 are 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.

We are recommending that the NASA Administrator implement an effective agencywide security program that includes improvements in five categories: assessing risks and evaluating needs, implementing policies and controls, monitoring compliance with policy and effectiveness of controls, providing computer security training, and coordinating responses to security incidents. NASA concurs in all of our recommendations.

[2] Executive Guide Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

Background

NASA depends heavily on IT to support the operations it conducts at its 10 field centers and associated facilities across the United States. NASA uses IT to maintain and operate the space shuttle; design, build, and operate the International Space Station; remotely control advanced scientific satellites such as the Mars Pathfinder; and develop critical new aeronautical technologies for use on next-generation aircraft. NASA estimates that it spent about $1.7 billion of its total appropriation of approximately $14 billion in fiscal year 1998 on IT.

Many of NASA's systems are extensively interconnected through the Internet, both within and outside of NASA, and can be an attractive target for individuals and organizations desiring to learn about or damage NASA's operations, including would-be hackers as well as industrial spies and foreign intelligence agents. With little technical skill and knowledge, a potential intruder can mount sophisticated attacks on systems connected to the Internet. Many known vulnerabilities of common operating systems are publicly posted on the Internet, and software tools for exploiting these vulnerabilities, written by skilled hackers, are freely available over the Internet.

NASA formally established its IT security program in 1979 by issuing its first agencywide policies regarding the security and integrity of agency computing facilities. Since 1995, NASA's Chief Information Officer (CIO) has had overall responsibility for setting and enforcing IT security policy and standards. The CIO discharges this responsibility by relying on an IT security program manager at Ames Research Center in Moffett Field, California, to interact with officials throughout NASA to identify security issues and propose new policies and standards. Policies and standards are adopted after consensus is reached among representatives of NASA's program offices and field centers.

Objectives, Scope, and Methodology

Our objectives were to determine (1) whether NASA's mission-critical information systems are vulnerable to unauthorized access, (2) whether NASA is effectively managing information systems security, and (3) what NASA is doing to address the risk of unauthorized access to mission-critical systems.

To determine whether NASA's mission-critical information systems are vulnerable to unauthorized access, we conducted controlled penetration tests of systems at one NASA field center that hosts a number of mission-

critical systems. At NASA's request, we arranged with the National Security Agency (NSA) to assist in testing and evaluating the agency's technical controls for ensuring that data and systems at this field center are protected from unauthorized access. We determined the scope of the tests NSA conducted, monitored their progress, and reviewed their work papers. We informed NASA in advance of all tests to be conducted, and obtained their concurrence. All testing was physically monitored by NASA personnel, who were authorized to halt testing once we obtained access to sensitive information or systems. We limited the testing to unclassified, mission-critical systems agreed upon in advance with officials from the field center. At the conclusion of our testing, we provided senior NASA managers with the test results and recommendations for correcting the specific weaknesses identified.

To evaluate whether NASA is effectively managing information systems security, we reviewed official documentation and held discussions with key agency officials responsible for the IT security program, including the CIO and the IT security program manager. We reviewed NASA's practices in comparison with the Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources, which was last updated in February 1996. We also compared NASA's practices to guidelines in two National Institute of Standards and Technology (NIST) publications, Generally Accepted Principles and Practices for Securing Information Technology Systems (Spec. Pub. 800-14, September 1996) and An Introduction to Computer Security: The NIST Handbook (Spec. Pub. 800-12, October 1995). In addition, we interviewed officials from NASA's Office of Inspector General and reviewed recent Inspector General reports on computer security at NASA.

We also used our May 1998 Executive Guide. Our guide identifies key elements of an effective information security program and practices that eight leading nonfederal organizations have adopted and details the management techniques these leading organizations use to build information security controls and awareness into their operations. This guide has been endorsed by the federal government's CIO Council, which is chaired by OMB's Deputy Director for Management. It describes a framework for an effective IT security program based on the following five risk management principles:

- assessing risk and determining needs,
- establishing a central management focal point,

- implementing appropriate policies and related controls,
- promoting awareness, and
- monitoring and evaluating policy and control effectiveness.

To determine what NASA is doing to address the risk of unauthorized access to mission-critical systems, we requested and obtained specific information from the CIOs at each of NASA's 10 field centers on security for their mission-critical systems. We focused our efforts on the following categories of mission-critical systems: (1) applications and networks that are involved with the development and operations of both manned and unmanned spacecraft, (2) applications and networks involved in the processing and interpretation of scientific data obtained from space missions, and (3) applications and networks involved in the development and testing of aeronautics and space transportation technologies. We reviewed center-specific IT security policies, guidance, and information provided by the field center CIOs for 155 systems that they reported as falling into our mission-critical system categories. This information included security and contingency plans, risk assessment reports, IT security self-assessments and audit reports, and system authorizations. We determined whether NASA's practices were in compliance with OMB and NIST guidance as well as NASA's own policy. We did not attempt to verify the completeness or accuracy of the information provided by the field center CIOs.

We performed our audit work at NASA headquarters and five field centers from August 1997 through December 1998 in accordance with generally accepted government auditing standards.

Mission-Critical System Targeted in Our Tests Were Vulnerable to Unauthorized Access

With nothing more than publicly available Internet access, we performed penetration testing at one of NASA's 10 field centers, simulating outside attackers. Our test team was able to systematically penetrate systems involved in two mission-critical functions: (1) supporting the command and control of spacecraft and (2) processing and distributing scientific data returned from space. The systems supporting the command and control of spacecraft were involved in determining and verifying a variety of detailed spacecraft positioning data, such as orbital attitude (the precise orientation of a spacecraft with respect to the earth) and other orbit information used in planning spacecraft maneuvers and establishing and maintaining communications with ground controllers. This information is also used by scientists in analyzing and interpreting data collected by orbiting spacecraft as well as in planning for future data collection. The systems

involved in processing and distributing scientific data returned from space serve as electronic staging areas for data recently collected from space. Data transferred to these systems are processed to make them useful to scientists and then distributed to the scientific community.

We initially penetrated these systems using easily guessed passwords that provided limited access to certain parts of these systems. This limited access allowed the test team to observe and record the passwords to other accounts and search out further flaws, such as well-known operating system security holes, that led to broader access. Having obtained this broader access, we could have stolen, modified, or deleted important operational data, damaged operational information systems, or disrupted ongoing space flight operations.

We could not penetrate all the systems we attacked. In particular, 2 of the 11 organizations at the field center where we performed penetration testing managed the security of their systems more effectively than the others, preventing us from penetrating their systems within the time and resources available. For example, one network appeared to control system access privileges carefully and had "patched" operating system software for well-known flaws. Another network used a strong user authentication technique that made it impossible to gain access by using passwords from compromised accounts. [3] As a typical hacker would most likely do, our test team did not spend additional time attempting to compromise these apparently robust systems but instead moved on to other systems with easily exploitable weaknesses.

Vulnerabilities Encountered During Our Penetration Tests

The vulnerabilities encountered during our tests fall into four major categories: (1) poorly chosen passwords, (2) inadequate data access controls, (3) system software patches not kept up to date, and (4) unnecessarily broad trust relationships among networked systems. By exploiting a combination of these vulnerabilities, our team was able to gain access to a single computer in a given network, gradually increase their control of that machine, and use this to access other computers on the same networks and on interconnected networks.

[3] Strong user authentication refers to techniques to validate the identity of a user based on sophisticated technology that is significantly more difficult to defeat than simple password-based approaches.

Poorly chosen passwords provided the penetration team with easy access to individual computers. The team discovered passwords that were relatively easy to guess, such as "guest" for guest accounts. They also found that system administrators had chosen obvious passwords, such as "adm" or "administrator" for their own accounts and had assigned "changeme" or "newuser" as temporary passwords for new users, who in turn never bothered to replace them with unique passwords. In some cases, standard dictionary words or common names were used as passwords and thus were easily guessed by password cracking software, which is freely available over the Internet. Other accounts were found with passwords that were easily derived from users' names. For example, if an account was assigned to "John Jones," the password was easily guessed to be "jjones." Worse still, some accounts had no passwords at all.

In addition, many of these systems were not set up to restrict access to key data, such as file directories that contained vital computer configuration data or users' individual file directories. Not setting restrictions on access to such data makes it easier for system administrators to manage file sharing among groups of colleagues; however, it also makes such systems extremely vulnerable to unauthorized intrusion. Having gained access to the system by guessing a poorly chosen password, the team could then read or alter key data files in any of the unrestricted file directories, including the system's password file. The penetration team could then appear to the system as any authorized user it chose, including the system administrator, and could have destroyed all of the software and data resident on the computer.

The team also exploited well-known security flaws in commercial off-the-shelf system software to gain unrestricted access to systems and data. When flaws are discovered in publicly released versions of system software, hackers often respond by producing and posting to the Internet easy-to-use software tools that exploit the newly discovered vulnerability. These tools are then readily available to other attackers. To foil this tactic, it is vital that system administrators keep up to date with known system flaws, test their computers for vulnerability, and install the latest system software patches, which are also often freely available on the Internet. System administrators at the tested center did not consistently patch their systems to correct well-known flaws. For example, our penetration team found old versions of Sendmail, a commonly used electronic mail program with a well-known flaw, running on several of NASA's computers. Because the software had not been patched, we exploited the flaw to gain access to these systems.

Finally, the team found unnecessarily broad trust relationships among NASA's networked computers. A "trust relationship" allows users of one system to freely access other systems in the relationship, as if those other systems were simply extensions of the user's home system. Thus, a hacker who gains access to one system in such a relationship can then access all the other systems that trust it. While trust relationships are of great practical importance when working in a networked environment, they need to be carefully managed because of the risk they pose. Some of the systems we tested were not carefully managed in this regard. For example, the team found that one of the targeted computers that we successfully penetrated was trusted to access as many as 89 other systems. Since by gaining access to one trusted system the team could get access to all others, this one "weak" system undermined the security of the entire group. In order to reduce this vulnerability, the risks and benefits of trust relationships need to be carefully analyzed before the relationships are established.

Modem Connections Could Allow Intruders To Circumvent Access Controls

Dial-in modem connections can pose serious risks to computer systems because they can allow an intruder to circumvent access controls such as firewalls and intrusion detection software that protect a network from external threats. For this reason, NASA has a policy restricting the connection of modems to mission-critical systems. However, NASA has no assurance that this policy is effectively implemented since it has no agencywide procedures for either registering modem lines when they are installed or systematically tracking down unauthorized modem connections. For example, when the penetration team found a number of potentially active modem connections using a "wardialer," [4] NASA officials had no way of identifying to which systems these lines were connected. NASA did not maintain a master list of authorized modem lines. As a result, it could not determine whether mission-critical systems were accessible through unauthorized modems.

[4] A wardialer is a program, readily available over the Internet, that dials a range of telephone numbers to identify those belonging to modems or other electronic devices.

Management of NASA's IT Security Program Has Been Ineffective

A major contributing factor to our ability to penetrate mission-critical systems at NASA is that the agency was not effectively and consistently managing IT security. While some of NASA's mission-critical systems had effective security controls, other equally critical systems had inadequate protection.

We found management deficiencies at NASA in the following areas: (1) assessing risks and evaluating needs, (2) implementing policies and controls, (3) monitoring and evaluating the effectiveness of policies and controls, (4) providing computer security training to employees, and (5) establishing a central IT security staff to coordinate responses to security incidents.

NASA Does Not Effectively Assess Risks Or Evaluate Needs

Federal guidance requires all federal agencies to develop comprehensive IT security programs based on assessing and managing risks. [5] The objective of risk-based security management is to develop an IT security program that represents an optimal investment of limited resources—neither overspending on technical measures that may not be warranted given the nature of the threat nor underprotecting critical information that has significant known vulnerabilities. To achieve that goal, managers must conduct valid risk assessments for their IT assets and accept responsibility for the adequacy of the security controls adopted to mitigate assessed risks.

NASA policy requires that risk assessments be conducted for all major systems prior to their becoming operational, upon significant change, or at least every 5 years. [6] Furthermore, NASA requires that these risk assessments address specific topics, including (1) the value and criticality of the assets, (2) the potential threats, (3) the exposure of the assets to risk, (4) the level of risk that would be acceptable, and (5) appropriate protective measures. However, 135 of the 155 systems that we reviewed did not meet all of these requirements. For example, risk assessments had

[5] The February 1996 revision to OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, requires agencies to use a risk-based approach to determine adequate security, including a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. Additional guidance on effective risk assessment is available in NIST publications.

[6] New guidance, now in draft form, will increase the required frequency to at least every 3 years, in conformance with OMB guidelines.

not been conducted within the last 5 years for 57 of the systems, potential threats had not been identified for 127 of the systems, and risk exposure had not been assessed for 81 of the systems.

NASA security officials are aware that the agency is not in compliance with either federal guidelines or NASA's own policy, and several internal security reviews have reported that the agency is not meeting minimum requirements for risk assessments. These reviews noted that two field centers were failing to identify threats and that four centers were not conducting assessments every 5 years, as required. A system security review conducted at one center, for example, reported that risk assessments were not used to determine what protective measures were appropriate for systems, and that there was no documented evidence that risk assessments had been conducted prior to declaring systems operational.

Furthermore, OMB Circular A-130 requires management officials to formally authorize use of a system prior to its becoming operational, upon significant change, and at least every 3 years thereafter, and recommends authorizing mission-critical systems even more often. By formally authorizing systems for operational use, managers accept responsibility for the adequacy of the security controls adopted to mitigate assessed risks. NASA managers, however, are not properly authorizing systems. Of the 155 systems in our sample, 133 had not been formally authorized for operational use.

The widespread lack of up-to-date and complete risk assessments indicates that many NASA managers have not carefully and systematically analyzed the threats and vulnerabilities of their IT systems and have not implemented security controls based on such analyses. Furthermore, there is little evidence that systems' managers have reviewed and accepted responsibility for the adequacy of the security controls implemented on their systems. As a result, NASA has no assurance that these systems are being adequately protected.

NASA Does Not Effectively Implement Policies and Controls

For policies to be effective, federal guidelines require agencies to frequently update their IT security policies in order to assess and counter rapidly evolving computer and telecommunications threats and vulnerabilities.[7] However, NASA has been extremely slow in updating its official agencywide IT security guidance. Although NASA issued an updated policy directive on IT security in October 1998, much of its

detailed guidance is dated 1993 and was developed before the explosive growth of the Internet and NASA's extensive use of it.

For example, NASA's outdated guidance does not specify what information can be posted on public World Wide Web sites, nor does it distinguish this from information that is sensitive and should be more closely controlled. We found that sensitive information, which could be used to facilitate a potential intruder's attempt to break into NASA systems, was publicly available through the World Wide Web. This included diagrams showing how NASA systems were connected to the Internet, names of system administrators and major users, Internet Protocol addresses, and telephone numbers for dial-up connections.

NASA officials have also noted this problem. A 1997 status report for one NASA network states: "the Center's recent push to make as much data available via the Web as possible has led to a proliferation of distributed and mostly unmanaged Web servers. This coupled with the Center's direction to put a server on every desktop has led to a security nightmare in which systems which were intended to make information available to the Center have unknowingly made it accessible to the world."

NASA's outdated guidance also does not specify how field centers should protect mission-critical systems from well-known Internet threats. For example, tools such as network "sniffers," which are freely available over the Internet, make it easy to compromise systems that are protected only by passwords. A network sniffer monitors legitimate users as they log on to network systems and records their identification codes and passwords, which can then be used to gain access to NASA mission-critical systems. Even "well chosen" passwords—passwords that are difficult to guess—provide no protection from sniffers, which can identify and record any unencrypted passwords. During our penetration tests, we used this technique to gain access to NASA mission-critical systems.

NASA's guidance does not specify criteria for determining which systems require a stronger form of authentication than passwords. Strong authentication technology is available commercially in a variety of products. These products use encryption and/or short-lived access codes which, if "sniffed," cannot successfully be reused. During our penetration

[7] The February 1996 revision to OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources.

tests, we encountered one NASA system that used strong authentication. We could not access that system, even though we observed users logging in to it, because the short-lived access codes we could collect were not valid for reuse. However, we successfully penetrated other equally critical systems, including those involved in the command and control of orbiting spacecraft, because they did not use strong authentication.

NASA's inefficient revision process contributes to its inability to keep its IT security policy current. Proposed revisions to policy are subjected to a lengthy review process that attempts to gain unanimous agreement among representatives from all of the agency's major programs and field centers. For example, NASA's draft IT security procedures and guidelines document has been in the policy review process for more than 2 years. Because technology and the nature of threats and countermeasures change quickly, NASA's slow process cannot effectively address the increasing risk to the agency's systems.

NASA Is Not Monitoring Policy Compliance Or Effectiveness of Controls

By periodically monitoring and enforcing compliance with IT security policies, management demonstrates its commitment to the security program, reminds employees of their roles and responsibilities, and identifies and corrects areas of noncompliance. For these reasons, OMB Circular A-130 mandates that the security controls of major IT systems be independently reviewed or audited at least every 3 years. This enables agencies to ensure that controls are functioning effectively and to correct identified deficiencies .

NASA is not periodically monitoring its field centers to determine whether they are complying with agencywide policies. NASA has not conducted an on-site agencywide review of IT security since 1991, the last year that teams from headquarters visited the field centers to conduct management reviews. Six years ago, as a money saving initiative, NASA discontinued its periodic management reviews. Instead, it recommended but did not require that field centers monitor and assess themselves. Without centralized monitoring, NASA has no assurance that its security policies are implemented consistently across the agency.

Moreover, NASA does not regularly conduct agencywide independent security audits and reviews. There was no record of any independent audit or review having been conducted for 60 percent of the mission-critical systems for which we obtained information. Furthermore, NASA is not consistently following up and correcting deficiencies identified in the

audits that are performed. Thirty-seven of the 155 systems for which we reviewed audit reports had recurring deficiencies. For example, a 1989 audit reported that the computer audit trail software for a major system at one field center had been disabled. As a result, for this system, the center could not ensure individual accountability, reconstruct events, detect intrusions, or identify problems. This deficiency was reported again in 1992 and yet again in 1994.

Without monitoring its systems, requiring independent periodic audits and reviews, and correcting identified weaknesses, NASA management cannot ensure that its IT security policies are being consistently implemented across the numerous systems located at its field centers. Nor can it ensure that the security controls that are implemented on these systems continue to be effective.

NASA Is Not Providing Required Computer Security Training

The Computer Security Act of 1987 mandates that all federal employees and contractors who are involved with the management, use, or operation of federal computer systems be provided periodic training in IT security awareness and accepted IT security practice. Specific training requirements are contained in NIST's training guidelines, which establish a mandatory baseline of training in security concepts and procedures and define additional structured training requirements for personnel with certain security-sensitive responsibilities. For example, in addition to baseline training, systems administrators, who are responsible for ongoing day-to-day system use and maintenance, require training to enable them to identify, analyze, and evaluate potential security incidents in order to maintain appropriate safeguards. Similarly, program managers, who must authorize a system for operation, need to be trained to identify threats and vulnerabilities and evaluate the adequacy of controls.

NASA has no structured security training curriculum, as required by federal guidelines. According to the 1998 special review of its IT security program, NASA training is currently carried out on a "hit or miss basis," with activities varying from center to center and supported by limited funding and staff. Moreover, NASA has no assurance that its contract employees are adequately trained. NASA regulations prohibit the expenditure of government funds to train contract employees, and NASA does not require that its contractors complete specific training programs. Since as many as 90 percent of NASA's system administrators are contractors, NASA has no assurance that many of its personnel involved in IT operations are adequately trained.

Our review of NASA risk assessments and audit reports cited inadequate IT security training as a problem at 7 of the 10 NASA field centers. A 1996 audit report from one field center, for example, states:

> "In general, the responses to all questions concerning documented protection/security procedures were vague and failed, in most cases, to identify documented practices. There is little indication that [required security controls] are in place or even commonly known. There appears to be little organizational discipline in the formulation, awareness, and adherence to computer security/protective measures. This creates serious vulnerabilities while allowing for little accountability. "

In 1997, the Glenn Research Center was assigned responsibility for assessing NASA training and developing a NASA-wide training curriculum. Responsible officials from Glenn characterized the level of training throughout the agency as "abysmal." They stated that few systems administrators have received any IT security training at all. Further, they stated that NASA program managers, who are supposed to be assessing risks to their systems based on threat and vulnerability, are "blindly accepting risks" because they have never been trained in the risk management process. Even IT security officers throughout NASA, they concluded, need more and better training. The Glenn officials have prioritized needed IT security training activities and have begun developing a core curriculum.

The Office of the NASA CIO has recently developed a 50-minute computer-based IT security awareness module, which is scheduled for distribution sometime this year. The targeted audience of this training is system users and it emphasizes such countermeasures as using strong passwords. Headquarters is planning to develop additional modules to cover the more technical training required of systems administrators, program managers, and IT security officers, but program officials project that it will be at least 2 years before they are in place.

NASA Does Not Effectively Coordinate Responses to Security Incidents

OMB Circular A-130 requires agencies to establish central organizations dedicated to evaluating and responding to security incidents and sharing information concerning vulnerabilities and threats with other officials and organizations, such as managers at other agency sites, other federal agencies, incident coordination groups, and law enforcement agencies. Once an intrusion or other security incident is detected, it must be reported to the central organization. If the central organization determines that a vulnerability exists, it can identify corrective measures and can alert other

organizations, both internally and externally, to the vulnerability and its repair.

In 1993, NASA established a centralized agency-level organization, the NASA Automated Systems Incident Response Capability (NASIRC), to assist in carrying out agencywide computer security incident detection and coordination. However, during our audit we found that field centers were not reporting incidents to NASIRC. Although NASA is subjected to thousands of attempted computer system penetrations every month, between January 1994 and April 1997, fewer than seven such incidents per month, on average, were reported to NASIRC.

The lack of comprehensive central reporting undermines NASIRC's ability to track agencywide trends and assess the threats of greatest concern so that adjustments to security controls can be made as needed. Furthermore, when an attack on NASA's systems has occurred or is taking place, the lack of consistent and comprehensive reporting limits NASA's ability to effectively ascertain the extent to which security has been compromised and to respond appropriately.

NASA Is Considering Improvements Consistent With Our Management Framework

The NASA Office of Inspector General has repeatedly questioned the adequacy of NASA's IT security program, and in February 1998 we discussed some of our preliminary findings about information security with NASA IT security officials. In response to these concerns, NASA initiated a special review of its IT security program in May 1998 that included the use of our Executive Guide as criteria. NASA's review identified a number of shortcomings that are consistent with our findings and made a series of 33 recommendations, including the following:

- immediately issue the revised policy and guidance documents that had been in draft for more than 2 years,
- fund, develop, and implement an IT security certification program and other IT security training programs,
- clarify the role of NASIRC and organize an incident response system to provide real-time coordination of assistance during network incidents, and
- determine administrative sanctions for noncompliance with IT security regulations.

Although the NASA CIO has developed a 2-year plan for addressing shortcomings in the agency's program, at the time of our review NASA had

not implemented most of the special team's recommendations, including those cited above. For example, a new NASA policy document on IT security was issued in October 1998, but its much more extensive companion document, which provides detailed guidance, was still in draft. The CIO's office sponsored development of an instructional CD-ROM that is intended to provide basic awareness of IT security for all NASA employees, but NASA hadn't yet developed the recommended training and certification program. Finally, no action had been taken to determine administrative sanctions for noncompliance with IT security regulations.

Conclusions

Many of NASA's mission-critical systems are vulnerable to unauthorized access and sabotage and their data to theft, modification, and destruction. This is in large part due to significant management shortcomings in every aspect of NASA's IT security program, including assessing risks, implementing policy, monitoring and evaluating policies and controls, training employees, and centrally coordinating responses to security incidents. NASA recognizes that it needs to improve its IT security program and conducted a special review of IT security, but, at the time of our evaluation, had not implemented most of the recommendations made in its review. Until it establishes a comprehensive IT security management program, NASA will be unable to ensure that its IT assets are adequately protected.

Recommendations

We recommend that the NASA Administrator, with support from NASA's CIO, implement an effective IT security program that is consistent across NASA's field centers and incorporates the following key elements:

- Assessing risks and evaluating needs, which includes the following:
  - Developing and instituting a review process to ensure that managers conduct complete risk assessments for all major systems prior to the systems becoming operational, upon significant change, or at least every 3 years.
  - Formally authorizing all systems before they become operational and at least every 3 years thereafter.
- Implementing policies and controls, which includes the following:
  - Streamlining the policy-making and standards-setting process for IT security so that guidance can be issued and modified promptly to address changes in threats and vulnerabilities introduced by rapidly evolving computer and telecommunication technologies.

    - Developing and issuing guidance that specifies information that is appropriate for posting on public World Wide Web sites and distinguishes this from information that is sensitive and should be more closely controlled.
- Developing and issuing guidance that identifies critical systems, including those involved in the command and control of orbiting spacecraft, that require strong user authentication.
- Monitoring compliance with policy and effectiveness of controls, which includes the following:
    - Developing and implementing a management oversight process to periodically monitor and enforce field centers' compliance with agencywide policy.
    - Ensuring that independent audits or reviews of systems' security controls are performed at least every 3 years and that identified weaknesses are expeditiously corrected.
- Providing required computer security training, which includes the following:
    - Developing and implementing a structured program for ensuring that NASA employees receive periodic training in computer security to provide them with the awareness, knowledge, and skills necessary to protect sensitive information and mission-critical systems.
    - Modifying relevant contracts to include provisions for ensuring that NASA contract personnel are similarly trained.
    - Developing and implementing a program for certifying that NASA civil servants and contract employees are competent to discharge their IT security-related responsibilities.
- Coordinating responses to security incidents, which includes the following:
    - Clarifying policy and procedures for mandatory reporting of security incidents to NASIRC.
    - Strengthening the role of NASIRC in disseminating vulnerability information within NASA, analyzing threats in real time, and developing effective countermeasures for ongoing attacks.

We also recommend that the NASA CIO review the specific vulnerabilities and suggested actions provided to field center officials at the conclusion of our penetration testing, determine and implement appropriate security countermeasures, and track the implementation and/or disposition of these actions.

Agency Comments and Our Evaluation

In written comments on a draft of this report, which are reprinted in appendix I, NASA's Associate Deputy Administrator stated that the report will be extremely useful to NASA in improving its IT security posture and concurred in all of our recommendations. However, NASA did raise two concerns. First, agency officials were concerned that a casual reader of the draft report could incorrectly conclude that all of NASA's mission-critical systems at all of its field centers could be penetrated, based on the statement that "NASA's mission-critical systems are vulnerable to unauthorized access and sabotage." We found that some NASA mission-critical systems are significantly better protected than others, and in some cases our penetration tests did not gain access to targeted systems. However, our testing showed that many mission-critical systems are indeed vulnerable. We have modified the report to clarify our point that many of NASA's systems are vulnerable.

Second, NASA stated that it is working diligently to implement the recommendations of its special review of IT security, referred to in our report. In a chart accompanying its comments, NASA synopsized its position on each of our recommendations, the actions it is planning to address those recommendations, and the associated timeframes for completion. The chart is included in appendix I. We are pleased with NASA's commitment to solving these problems. Effective corrective actions will be important because many of NASA's systems will remain vulnerable to unauthorized access until the agency successfully executes its plan and implements all of our recommendations.

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 5 days from the date of this letter. At that time we will send copies of this report to Senator Christopher S. Bond and Senator Barbara A. Mikulski, and to Representative Dan Burton, Representative Alan B. Mollohan, Representative James T. Walsh, and Representative Henry A. Waxman in their capacities as Chair or Ranking Minority Member of Senate and House Committees and Subcommittees. We are also sending copies of this report to The Honorable Daniel S. Goldin, Administrator of NASA. Copies will be available to others upon request. If you have questions about this report,

please contact me at (202) 512-6240. Major contributors to this report are listed in appendix II.

Jack L. Brock, Jr.
Director, Governmentwide
and Defense Information Systems

Comments from the National Aeronautics and Space Administration

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

APR 20 1999

Mr. Gene L. Dodaro
Assistant Comptroller General
United States General Accounting Office
Washington, DC 20548

Dear Mr. Dodaro:

Thank you for the opportunity to comment on GAO's draft report entitled "Information Security: NASA's Mission Critical Systems Face Serious Risks." We believe that your assessment of NASA's information security program was conducted in a most professional manner that will be extremely useful to the Agency in improving its Information Technology (IT) Security posture. We agree with many of your findings and concur in all the recommendations.

Enclosed is NASA's response to the issues raised in your report. We have not attempted to raise issues regarding relatively minor disagreements we have with some of the draft report's findings. Rather, we have focused on two concerns, one of which could lead to possible misinterpretation of the vulnerability to penetration of NASA's systems, and the second to a misunderstanding of NASA's commitment to improving its IT Security program.

NASA's review of the subject report required an approximate aggregate of 500 staff hours. If you have any questions regarding NASA's comments or would like to discuss them further, please contact Carmela Simonson on (202) 358-1223 to make the necessary arrangements.

Sincerely,

J.R. Dailey
Associate Deputy Administrator

Enclosure

NASA Comments on GAO Draft Report Entitled
"Information Security: NASA's Mission Critical Systems Face Serious Risks"

NASA has reviewed the draft GAO report and agrees with many of the findings and all of the recommendations. We find the GAO audit to be very useful to the Agency in that it both reinforces the recommendations made by our recent Agencywide Information Technology (IT) Security review and provides additional ones which will assist in better protecting NASA's IT assets. We appreciate the professional quality of the GAO review and the productive working relationship established between the auditors and NASA officials.

NASA does have two concerns regarding the report. First, a casual reading of the Conclusions section of the report could lead to a misinterpretation of the statement that "NASA's mission-critical systems are vulnerable to unauthorized access and sabotage." This statement could be misunderstood to mean that all of NASA's mission-critical systems at all of its Centers could be penetrated. In fact, the report states that penetration testing was unsuccessful in several cases. Penetration testing of a limited number of systems at one Center cannot be extrapolated to all of NASA's mission-critical systems at all of its Centers.

NASA does take extraordinary steps, not noted in the study, to protect certain systems and networks prior to events such as launches. We believe that these steps are very effective, but due to increasing capabilities and motivation of those who would do harm to NASA, we are not complacent and continue to make improvements. NASA takes very seriously the GAO findings in the area of IT Security management, and we will correct our deficiencies. We agree that the Agency must manage IT Security more effectively and by doing so will provide better protection for all of our mission-critical systems.

The second concern is that because the GAO audit, like any audit, is a snapshot in time, the reader may conclude that NASA is doing little to improve its IT Security posture. We are far from indifferent to IT Security which, after the Year 2K effort, is our highest priority. As a result, we are working diligently to implement the 33 recommendations made in our Agencywide IT Security review. GAO is correct that some of our recommendations will take 2 years to implement. That is largely because we are making fundamental improvements in the skills of both our civil service personnel and contractors. Suitable training curricula in some areas, for example, are just now becoming available. We believe the result will be worth the required investment in time and resources, and we are making that investment.

NASA is also taking near-term action to make the following improvements:

- In December 1998, we purchased Public Key Infrastructure (PKI) digital certificates for every NASA employee that will allow us to encrypt sensitive

data, provide digital signature capabilities, and perform strong authentication. We are implementing the PKI capabilities Agencywide this fiscal year.

- This fiscal year, we are purchasing and implementing Agencywide a common set of auditing and monitoring tools that will allow us to better monitor the security status of our systems, better detect intruders, and, because the tools are common, better coordinate our response to attacks against multiple Centers.
- In October 1998, the NASA Administrator issued a letter to Center Directors reinforcing the policy concerning reporting of IT Security incidents to NASA Automated Systems Incident Response Capability (NASIRC). Shortly thereafter, the NASA CIO provided additional, detailed guidance in this regard to the Center Directors. Incident reporting to NASIRC is improving as a result, but we continue to require better compliance in this area.
- This fiscal year, we are beginning penetration testing between Centers to allow us to determine, through testing much like GAO conducted at one NASA Center, the effectiveness of NASA's protection of its IT assets. We will use the lessons-learned from this year's experience to both better secure our systems and perform independent penetration tests in succeeding years.
- NASA's IT Security training plan is currently under review by the Centers and training offices, and we expect that it will be approved soon. As noted in the GAO report, in 1998 NASA developed a multimedia CD-ROM which we believe provides excellent IT Security awareness training. We have distributed the CD-ROM to all the Centers.
- NASA's revised, detailed IT Security guidance is nearing completion and will be issued shortly.
- We are conducting IT Security workshops on a regular basis so that the Center IT Security Managers, network engineering/operations personnel, and outsourcers can exchange information and develop approaches to improving NASA's IT Security.

NASA believes that the actions taken since the completion of the GAO audit, those that are in process and planned as a result of our Agencywide review, and those initiated as a result of the GAO review will make NASA a leading agency in IT Security. We acknowledge the timely assistance that GAO has provided in this regard by the assessment documented in its draft report.

Following is our detailed response to the specific recommendations provided in the GAO draft report.

Specific Response to GAO Recommendations

NASA concurs with all the recommendations of the GAO report. The table below provides our response for specific elements of the first high-level GAO recommendation: "We recommend that the NASA Administrator, with support from NASA's CIO, implement an effective IT security program that is consistent across NASA's field centers and incorporates the following key elements:"

Recommendation	Concur?	Corrective Actions	Projected Timeframe for Completion
1. Assessing risks and evaluating needs, which includes the following:	Y		
a. Developing and instituting a review process to ensure that managers conduct complete risk assessments for all major systems prior to the systems becoming operational, upon significant change, or at least every 3 years.		During the last quarter of FY 1998, we implemented, and the revised detailed IT Security guidance (NPG 2810) will reinforce, the requirement for reporting of metrics in this area to the NASA IT Security Principal Center who presents the information to the NASA CIO. Metrics will be collected each quarter. In addition, consistent with the NASA management model, we will require Center Directors, working through Center CIO's, to implement a review process to ensure that the risk assessment policy, as with all IT Security policies and procedures, is adhered to at their Centers.	NPG 2810 issue: 3rd Quarter, FY 1999 Letter to Center Directors stating responsibilities in IT Security area: 3rd Quarter, FY 1999
b. Formally authorizing all systems before they become operational and at least every 3 years thereafter.		NPG 2810, when issued, will include this requirement. Metrics will be collected each quarter.	NPG 2810 issue: 3rd Quarter, FY 1999

Recommendation	Concur?	Corrective Actions	Projected Timeframe for Completion
2. Implementing policies and controls, which includes the following:	Y		
a. Streamlining the policy-making and standards-setting process for IT security so that guidance can be issued and modified promptly to address changes in threats and vulnerabilities introduced by rapidly evolving computer and telecommunication technologies.		Since NPG 2810 has taken longer to implement than we had planned, we have issued a number of management letters giving guidance in specific areas that required immediate attention. We will develop and implement a more streamlined process for IT Security guidance to supplement our existing policy process.	4th Quarter, FY 1999
b. Developing and issuing guidance that specifies information that is appropriate for posting on public World Wide Web sites and distinguishes this from information that is sensitive and should be more closely controlled.		NASA will issue guidance in this area. Since one of NASA's primary missions is dissemination of knowledge to the American public, our policy must be carefully crafted to ensure that we are excluding, from World Wide Web posting, only that information that must be kept from public dissemination. We must take the time necessary to develop appropriate guidance consistent with our mission.	4th Quarter, FY 1999
c. Developing and issuing guidance that identifies critical systems, including those involved in the command and control of orbiting spacecraft, that require strong user authentication		NPG 2810, when issued, will include this guidance. Consistent with OMB A-130 and NASA's approach to unclassified IT Security, guidance in this area will be based on risk assessments.	3rd Quarter, FY 1999

Recommendation	Concur?	Corrective Actions	Projected Timeframe for Completion
3. Monitoring compliance with policy and effectiveness of controls, which includes the following:	Y	Consistent with the NASA management model, we will require Center Directors, working through Center CIO's, to implement a review process to ensure that all IT Security policies and procedures, including those related to audits/ reviews and correction of weaknesses, are adhered to at their Centers. Metrics will be collected each quarter and reported to the Principal Center for IT Security and to the NASA CIO to monitor Centers' compliance with Agencywide policy.	Letter to Center Directors stating responsibilities in IT Security area: 3rd Quarter, FY 1999.
a. Developing and implementing a management oversight process to periodically monitor and enforce field centers' compliance with agencywide policy			
b. Ensuring that independent audits or reviews of systems' security controls are performed at least every 3 years and that identified weaknesses are expeditiously corrected			

Recommendation	Concur?	Corrective Actions	Projected Timeframe for Completion
4. Providing required computer security training, which includes the following:	Y	NASA's IT Security Training plan is at this time under concurrent review by the NASA CIO, Center CIO's, and the NASA training officers. The actions and schedule for compliance with this recommendation may change as a result of the review process.	
a. Developing and implementing a structured program for ensuring that NASA employees receive periodic training in computer security to provide them with the awareness, knowledge, and skills necessary to protect sensitive information and mission-critical systems.		Our IT Security training approach includes two components: (1) end-user awareness and training, training for program/project managers in risk management (including risk analysis), and training for Center IT Security Managers; (2) training for civil service and contractor system/network administrators which we interpret to be GAO recommendation 4.c. The time-frame for this recommendation refers to the first component.	4th Quarter, FY 2000 Intermediate milestones exist/under development for implementation of portions of the program and training percentages of users.

Recommendation	Concur?	Corrective Actions	Projected Timeframe for Completion
4. Providing required computer security training, which includes the following:	Y	NASA's IT Security Training plan is at this time under concurrent review by the NASA CIO, Center CIO's, and the NASA training officers. The actions and schedule for compliance with this recommendation may change as a result of the review process.	
b. Modifying relevant contracts to include provisions for ensuring that NASA contract personnel are similarly trained.			Modification of existing contracts: 3rd Quarter, FY 2000. Language for inclusion in new contracts to be developed in 4th Quarter, FY 1999.
c. Developing and implementing a program for certifying that NASA civil servants and contract employees are competent to discharge their IT security-related responsibilities			All civil service and contractor system/ network administrators: 3rd Quarter, FY 2001 50% of all civil service system/network administrators: 4th Quarter, FY 2000

5. Coordinating responses to security incidents, which includes the following:	Y		
a. Clarifying policy and procedures for mandatory reporting of security incidents to NASIRC		This action was completed via a letter from the NASA Administrator to the Center Directors in October 1998. A subsequent letter from the NASA CIO provided more details in this regard.	Clarification of policies is complete. Clarification of procedures will be provided in NPG 2810, when issued: 3rd Quarter, FY 1999
b. Strengthening the role of NASIRC in disseminating vulnerability information within NASA, analyzing threats in real time, and developing effective countermeasures for ongoing attacks.		This action is in progress as a result of our Agencywide IT Security Program Review. Improvements will be incremental with some aspects of the action in place before the completion date noted.	4th Quarter, FY 1999

The second high-level GAO recommendation is: "We also recommend that the NASA CIO review the specific vulnerabilities and suggested actions provided to field center officials at the conclusion of our penetration testing, determine and implement appropriate security countermeasures, and track the implementation and/or disposition of these actions". The NASA CIO has already reviewed the vulnerabilities and suggested actions GAO provided to field center officials and has met with the field center director to discuss vulnerabilities and the need for corrective action. The field center has already corrected a number of the vulnerabilities reported and is in the process of repairing those that remain. The NASA CIO will conduct a review of the field center's progress in this regard by June 15, 1999, and will track the implementation and/or disposition of remaining actions.

Major Contributors to this Report

Accounting and Information Management Division, Washington, D.C.

Rona B. Stillman, Chief Scientist
David L. McClure, Associate Director
Keith A. Rhodes, Technical Director
John A. de Ferrari, Assistant Director
Elizabeth L. Johnston, Evaluator-in-Charge
David F. Fiske, Senior Evaluator

Denver Field Office

Jamelyn A. Smith, Senior Information Systems Analyst

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00