Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

U.S. House of Representatives

For Release on Delivery
expected at
10:00 a.m. EDT
Tuesday
June 24, 2003

Cyber Security: The Status of Information Security and the Effects of the Federal Information Security Management Act (FISMA) at NASA

Statement of

The Honorable Robert W. Cobb

Inspector General

National Aeronautics and Space Administration

Mr. Chairman, Ranking Member, and Members of the Subcommittee:

Thank you for the opportunity to discuss information security at NASA and the impact of the Government Information Security Reform Act (GISRA) and the Federal Information Security Management Act (FISMA) on the Agency's information security program.

My statement focuses on three areas:

- Key information technology (IT) security challenges faced by NASA and its actions and plans to address them.
- Our audit of the information NASA submitted to the Office of Management and Budget (OMB) under GISRA in fiscal year (FY) 2002.
- Our plans to audit the information submitted by NASA under FISMA in FY 2003.

Before discussing these areas, I want to highlight some of the unique challenges associated with securing NASA's IT resources and how they are inextricably linked to the complex mission and operating structure of the Agency.

The NASA vision and mission concern challenges for scientific exploration and discovery. NASA pursues these challenges with a broad array of science programs, research and development in aeronautics, and space exploration. These endeavors include solar system exploration; Astronomical Search for Origins; Earth Science; Biological and Physical Research; Aerospace Technologies; the Space Launch Initiative; Education Initiatives; Space Flight, including the International Space Station and the Space Shuttle; and the corporate and institutional infrastructure to support these programs.

NASA employs about 19,000 civil servants and has a much greater number of contractor employees working on NASA programs at 11 major installations (including Headquarters, the 9 Centers, and the Jet Propulsion Laboratory). The Centers have diverse roles and historical cultures and, over time, have had substantial operational freedom in fulfilling mission objectives. NASA, like every other agency, faces a challenge in convincing its workforce that IT security is a primary rather than secondary responsibility.

The environment in which NASA IT systems operate provides a context and setting for understanding NASA's IT security challenges. The elements of this environment include:

- NASA has hundreds of programs requiring unique IT solutions.
- NASA's information security program is reliant on the judgment of all persons with access to sensitive information.
- NASA has a responsibility to protect varied types of sensitive and classified information.

- NASA carries out a civilian mission for which distribution of information about scientific exploration, discovery, and achievement is practiced by the Agency and expected and desired by the public.
- Contractors receive 90 percent of NASA dollars.
- NASA is a highly visible agency with many readily available Web sites, making it a natural target for those seeking to illegally access Government systems.
- NASA scientists and engineers focus on meeting specific program objectives and may not give sufficient attention to the IT security environment.
- NASA scientists and engineers often work in "open" educational environments with university scientists where "closed" information systems are an anathema.
- NASA maintains many institutional and mission-critical information systems for which security is critical in carrying out NASA programs and operations.

In my view, IT security comprises two elements: protection of information and protection of the IT resources that support information processing and storage. Information must be sufficiently protected to ensure confidentiality, integrity, and availability. Similarly, IT resources must be protected to ensure that hackers do not compromise them or programs that rely on them.

The requirements of GISRA and the recently enacted FISMA are having a positive effect on the state of IT security at NASA. The most positive impact has resulted from the laws' requirements to view the Agency's IT security posture as a whole, rather than as separate parts. The legislation and related OMB guidance have provided NASA with a framework for more effectively managing IT security. As a result, NASA senior management is increasing the attention given to IT security. The legislation also requires the Agency to consider the view of the Office of Inspector General (OIG) and to deal with issues raised in our independent evaluations.

NASA's unique mission and sophisticated operations present great challenges to those responsible for IT security. My office is committed to helping the Agency improve IT security through our ongoing program of IT audits and investigations.

THE STATE OF INFORMATION SECURITY AT NASA

Our December 23, 2002, report to the Administrator identified IT security as a significant management challenge. IT security activities at NASA have historically been carried out on a decentralized basis. This has resulted in a lack of synchronization in development efforts and a lack of full interoperability among the systems developed. We have reported on issues including inadequate security training for system administrators, an inconsistently applied program for ensuring security of sensitive systems, inadequate implementation of NASA's host and network security policies and procedures, inadequate security plans for NASA's IT systems, and an inadequate incident response capability. The independent public accountant responsible for NASA's FY 2002

financial statement audit identified several IT security deficiencies relating to the general controls environment over NASA's IT architecture that processes financial applications.

The previous NASA Acting Chief Information Officer (CIO) concluded in a briefing to the OIG on September 3, 2002, that NASA's internal systems could not support e-government initiatives as envisioned in the President's Management Agenda. Among the reasons cited were unacceptable security vulnerabilities. OMB reports NASA's status as "red" for e-government, noting among other issues weaknesses in some areas of IT security including program management, implementation, and evaluation.

On the positive side, we believe that NASA's leadership has implemented several IT security improvements and is now formulating plans to address many of the IT security concerns we have raised in past audits and investigations. The most promising overall improvement has been the recognition by the former Acting NASA CIO and the current NASA CIO that IT security is a problem that NASA must effectively address. We believe these positive changes should help to improve NASA's overall IT security posture.

Centralization and Integration of IT Security Is Needed

The implementation of security solutions is individual to NASA Centers and is not enterprise-wide. NASA is moving toward a OneNASA concept, with plans to implement a governance model that moves to a more centralized and integrated method of operating. NASA also plans to revise its IT security architecture. If implemented correctly, centralization and a revised architecture will improve the Agency's information security posture. However, as long as NASA governance structure is such that Center CIOs and security officials report to Center Directors—who are program officials—rather than to the NASA CIO and the Agency's Assistant Administrator for Security Management and Safeguards, a fully integrated approach to information security will be impossible at NASA.

Responsibility for overall IT security at NASA is divided between two organizations. For all unclassified systems, the Office of Security Management and Safeguards has responsibility for IT security policy and oversight, while the Office of the CIO has responsibility for IT security operations, procedures, and guidance. For classified systems, the Office of Security Management and Safeguards has responsibility for IT security policy, procedures, and guidance. These responsibilities for IT security have changed since NASA submitted its FY 2002 GISRA report. The FY 2002 report indicated that the NASA CIO maintained leadership of the entire IT security program.

NASA has established a Competency Center for IT Security (CCITS), currently the Ames Research Center in California. The CCITS is responsible for the technical coordination of information security implementation, the adoption of best security practices, information security consulting, and coordination of security incident reporting and analysis. NASA has integrated IT security into the Agency's capital planning and

investment control process. Furthermore, NASA's IT security program is integrated with its critical infrastructure protection responsibilities and other security programs. A Critical Infrastructure Protection Team is responsible for identifying NASA's critical cyber-based infrastructure assets.

NASA's Center Directors have oversight responsibilities for ensuring that an effective Center IT security program is established and maintained. Directors ensure compliance with Federal, Agency, and Center IT security policies, standards, and practices. Center IT Security Managers are appointed by the Directors to provide organization and direction for implementing the NASA IT Security Program at the Center level. Each Director appoints a Designated Approval Authority to accredit information resources for processing national security information. Centerwide IT security plans are approved by the Center Directors.

Each Center has a CIO responsible for establishing an effective and economical program at the Center. Senior organizational managers (e.g., Directorate Chiefs, Division Chiefs, Program Managers, Chief Financial Officer) have a role in supporting IT security planning, budgeting, and training. Each senior manager appoints a Computer Security Official who serves as a critical communication link to and from the organization for all IT security matters.

IT Security Weaknesses Identified in Recent Reports

We have an exceptional team of IT auditors, specialists, and computer crimes professionals who conduct audits of information security and perform investigations of the criminal misuse of NASA computers and attacks against the Agency's information and communication systems. Our aggressive pursuit of those responsible for illegal cyber activities outside and within the Agency is intended to serve as a deterrent. Because of the investment that the NASA OIG has made, we have been able to provide leadership in the IT and IT security areas to other OIGs. In my role as Chairman of the IT Roundtable for the President's Council on Integrity and Efficiency, I have sought to use my office's resources to promote the sharing of best practices in IT audits and investigations.

The General Accounting Office (GAO) designated computer security in the Federal Government as high risk in 1997. GAO continues to find evidence of pervasive weaknesses Governmentwide. The dramatic increase in computer interconnectivity and dependence on computers has, in part, caused such risks to increase. This year, GAO expanded this risk area to include protecting the information systems that support our nation's critical infrastructures.

During the course of an audit or investigation, our personnel often uncover systemic IT problems that are the root causes of compromises. Our recent activity covers a broad spectrum of security issues and criminal enterprises ranging from security training to

unauthorized access to sensitive information. Some examples of our work involving IT security at NASA follow:

Security Training

We continue to find that system administrators with responsibilities for system security have not received proper technical security training. We have linked inadequate technical training to security implementation problems in critical NASA systems. Individuals responsible for security administration must remain current with ever-changing technology. Without a trained and knowledgeable workforce, security administrators may not understand the vulnerabilities in the systems for which they have responsibility and may not be able to effectively secure them.

Implementation of Host and Network Security

We continue to find inadequate implementation of NASA's computer security policies in major NASA systems, including mission-critical systems. Contractor personnel manage most NASA systems with oversight from NASA. Inadequate security implementation can be attributed to a variety of problems, including unfamiliarity with NASA policy, differing interpretations of policy, inadequate training, and inadequate security tools. We have recently reported inadequate operating system and database security implementations and the need to strengthen firewall filtering, network monitoring, and other network controls.

Particularly noteworthy is our ongoing assessment of the use of wireless networks at NASA. Wireless networks are a versatile and efficient method for transferring data between computer systems. However, their use has several potential security risks. Our assessment to date has identified wireless networks in use at NASA that are not adequately secured. In large part, this was caused by the absence of an Agencywide policy to address wireless network security.

Incident Response Capability

NASA has established formal procedures for reporting security incidents for unclassified systems and for sharing information regarding common vulnerabilities. The procedures require the IT Security Manager at each NASA Center to report most incidents to the NASA Incident Response Center (NASIRC), which provides an Agencywide computer and network systems incident response and coordination capability. In turn, the NASIRC provides incident information to the Federal Computer Incident Response Center (FedCIRC), which is responsible for coordinating an incident response for Federal and civilian agencies.

We found that NASA Centers were not submitting all required reports on IT security incidents to the NASIRC. Thus, senior NASA IT security managers lacked incident information on an Agencywide basis, and NASA underreported and incorrectly reported incidents to the FedCIRC. Additionally, information in the NASIRC incident database

was unreliable for a variety of reasons, and the NASIRC could not produce accurate, complete, and meaningful analyses and reports. NASA agreed to address all OIG recommendations associated with this evaluation. Among the solutions proposed by the NASA CIO is one to shift the responsibility for identifying, reporting, and analyzing hostile probes to a centralized operation during FY 2003.

Unauthorized Access to Sensitive Information

There are examples from our ongoing investigations where inadequate IT security, such as weak password controls, resulted in unauthorized access to significant amounts of NASA data that was sensitive but unclassified. The Agency is aware of the cases and acknowledges that serious compromises have occurred. It would not be appropriate to share the details in any open forum.

Compromise of NASA and Department of Defense (DOD) Systems

Following the compromise of 15 NASA computer systems at 5 separate NASA Centers, we traced the attacks to a hacker in the United Kingdom. When NASA intrusion data was correlated with DOD data, it was determined that this hacker had compromised approximately 90 DOD computers. Based on a request from our office, authorities in the United Kingdom executed a search warrant in London and identified the hacker as Gary McKinnon. The Department of Justice (DOJ) is currently seeking McKinnon's extradition. We have been told that this is the first time DOJ has sought extradition for an alleged computer hacker.

Inconsistencies in Interpretation of NASA IT Security Guidance

On several occasions, we found that security weaknesses may be the result of inconsistent interpretations of NASA IT security guidance by the Centers. Of particular note was unclear guidance regarding IT security incidents and disaster recovery planning and testing. We reported that NASA disaster recovery planning and testing guidance did not define testing or describe the extent to which testing of the disaster recovery plan should be conducted. Without adequate guidance, NASA system managers test their systems to the extent they deem appropriate. We found that plans for mission-critical systems were sometimes tested less stringently than those for less critical systems. As a result, we recommended that certain guidance be clarified. NASA is currently updating and clarifying IT security guidance.

IT Security Performance Measures

We reported that improved performance measures were needed for vulnerability scanning, monitoring security throughout an IT system's life cycle, IT security plans, and incident response.

When performing vulnerability scanning, certain NASA Centers did not scan and obtain results on all IT systems. Some Centers adjusted their scanning results for exemptions

(known system vulnerabilities that were not corrected because the Center CIO had accepted the risk) and did not report them as required. As a result, NASA did not have an accurate vulnerability assessment of its networks.

Due to inadequate performance measures for monitoring security throughout an IT system's life cycle, NASA had limited assurance that its managers had considered specific risks and implemented appropriate controls for each life-cycle phase.

IT officials inaccurately reported to the NASA CIO that they had properly accomplished IT security plans for certain systems in accordance with NASA guidelines and OMB requirements. This decreased the NASA CIO's ability to effectively monitor and manage the Agency's IT security program.

NASA's FY 2002 incident response performance measure did not require the Agency to pass all of its test elements and was not comprehensive enough to fulfill the Agency goal to thwart intrusion attempts.

NASA's Actions and Plans to Address Key IT Security Challenges

NASA is making progress in improving IT security. The plan to establish a OneNASA governance model includes centralizing certain key security services and establishing a control process to ensure uniformity. Consolidation activities under the OneNASA architecture should also provide cost reductions. NASA plans to upgrade and standardize its IT security architecture to provide meaningful and realistic guiding principles and standards to be applied when designing and implementing information services for NASA users. This is a major step in the right direction.

Planning is underway to staff an assurance group within the Office of Security Management and Safeguards to validate that NASA IT security policy is being implemented. Current IT security guidance is being revised for clarity and to address new issues. NASA continues to deploy its Public Key Infrastructure (PKI) technology to perform encryption between applications on its networks and to resolve infrastructure and technical issues. This process has been slow. NASA also plans to enhance system vulnerability scanning and to deploy intrusion detection systems and rapid response capabilities to attempted break-ins.

NASA has also started a new program that requires all system administrators to be certified. This should result in the development of a consistent measure of the knowledge of their workforce. The measure is key to the implementation of appropriate IT security measures. NASA also plans to expand training to address IT security planning and risk analysis and to mandate various IT security courses for users, managers, and system administrators, as well as specialized courses for IT security personnel. Plans are also underway to make IT security and risk management a key component of system development activities. Finally, NASA is making progress in developing metrics for IT security performance and in instituting a comprehensive corrective action program

system to prioritize, track, and manage efforts to close security performance gaps and to support FISMA requirements. Whether all plans come to fruition remains to be seen. My office is committed to continued reviews of IT security. As part of our program, we will monitor and evaluate critical Agency remediation plans and results.

OIG REVIEW OF NASA'S FY 2002 GISRA SUBMISSION TO OMB

We performed numerous reviews relating to the Agency's unclassified IT security and infrastructure protection activities and used the results of those reviews in responding to OMB's FY 2002 reporting instructions. Additionally, we verified and validated the status of weaknesses identified in NASA's FY 2002 Plans of Action and Milestones (POA&M). Based on the results of our work, we suggested various changes to the Agency's draft submission. The Agency generally incorporated our suggestions into the final version submitted to OMB.

Our FY 2002 GISRA submission reflected the results of 26 final reports, 9 draft reports, and 2 ongoing assignments related to IT security at NASA. Our submission also reflected IT security-related work performed by the Agency's independent accountants as part of their annual review of NASA's financial statements. The reports and ongoing assignments addressed the following areas:

- NASA information systems processing national security information.
- The Agencywide IT security program for unclassified systems.
- NASA's planning and implementation for Presidential Decision Directive 63, "Protecting America's Critical Infrastructures," (Phase III).
- Capital planning for IT security.
- IT security requirements in NASA contracts, grants, and cooperative agreements.
- Performance management related to NASA IT security program goals.
- Approvals for accessing IT systems.
- UNIX security and integrity controls (various reports on individual NASA systems).
- Network firewalls.
- NASA's implementation of PKI.
- Internet-based spacecraft command security issues.
- NASA's Advanced Aeronautics Program.
- Removal of data from computer storage devices.
- NASA's incident response capability.
- Penetration testing at NASA.
- Management and control of authentication tokens.
- Operating system controls in a Space Shuttle problem-management system.
- NASA's implementation activities for critical cyber-based infrastructure assets (Phase II).
- IT security controls in NASA's financial management systems.

Our FY 2002 GISRA efforts were limited to unclassified systems because NASA did not provide the documentation that we needed to determine whether the Agency had complied with GISRA requirements pertaining to systems that process national security information. NASA management attributed its nonresponse to increased national security requirements caused by the September 11th terrorist attacks. NASA management stated that the National Security Agency had been unable to conduct its FY 2002 assessments of NASA's national security systems as a result of the increased workload on national security resources.

We also performed unique work to comply with OMB's GISRA reporting instructions including:

- We reviewed Center system inventories to determine whether they included both operational[1] and nonoperational[2] systems and whether the NASA CIO ensured that the Agency implemented its IT security plan throughout the life cycle of IT systems. We also asked the Centers to validate the inventories for completeness. Four of the 11 installations reviewed did not have an inventory of nonoperational systems. Of the remaining Centers that had inventory lists, we could not be assured that three of the system inventories contained all systems.

- We reviewed the Agency's progress in incorporating the NASA Federal Acquisition Regulation (FAR) Supplement 1852.204-76[3] in contractual documents to determine whether program officials used appropriate methods to ensure the security of contractor and other Agency-provided services. We also reviewed contractor operations related to host-based security, firewall[4] capabilities, authentication tokens, and removal of sensitive data from storage devices. We evaluated the Centers' and their contractors' efforts to reduce IT security vulnerabilities and reviewed a third-party's penetration testing activities.

[1] NASA Procedures and Guidelines 2810.1, "Security of Information Technology," identifies eight life-cycle phases. We defined operational systems as those in the final three phases: operations, upgrade, and disposal of assets at the end of their useful life.

[2] We defined nonoperational systems as those in the first five life-cycle phases: project initiation, project definition, design, construction, and installation/integration/testing.

[3] NASA FAR Supplement 1852.204-76 states that the contractor shall be responsible for IT security for all systems connected to a NASA network or operated by the contractor for NASA. The supplement also requires the contractor to provide, implement, and maintain a NASA-approved IT security plan; screen personnel requiring privileged access to systems operated by the contractor for NASA or interconnected to a NASA network; ensure its employees receive annual IT security training in NASA's IT policies and procedures; and incorporate the IT security clause in all applicable subcontracts.

[4] A firewall is designed to prevent unauthorized access to or from a private network. The firewall examines messages entering or leaving and blocks those that do not meet specified security criteria.

OIG PLANS TO VALIDATE THE NASA FY 2003 FISMA SUBMISSION TO OMB

During FY 2003, my office continued to conduct a series of IT security-related audits and assessments. As we did in FY 2002, we will incorporate the results of this work into our FISMA submission as well as any unique reporting requirements contained in OMB's FY 2003 reporting instructions for FISMA. We are conducting extensive follow-up work to determine whether weaknesses discussed in our FY 2002 GISRA report have been corrected. Finally, we will continue to review the Agency's POA&M prior to its submission to OMB. Ongoing FISMA-related audit work addresses the following areas:

- Database security and integrity.
- Information assurance controls for International Space Station software development and integration systems.
- Information assurance controls for engineering design systems supporting Space Shuttle ground operations.
- Information assurance controls for Space Shuttle launch test, control, and monitor systems.
- Security controls in NASA's Integrated Financial Management System.
- Information assurance controls in the Hubble Space Telescope Program.
- NT Security in a Center master domain.
- Information category designations in NASA systems.
- Security of wireless networks at NASA Centers.
- IT controls for NASA's FY 2003 Financial Statement Audit.

Also during FY 2003, we plan to start an audit of the adequacy of NASA policies to protect unclassified but sensitive information. We will address the adequacy of policies to prevent the unauthorized compromise of sensitive information, including disclosure, theft, destruction, alteration, and fabrication of information.

This concludes my formal statement. I will be pleased to answer any questions the Subcommittee may have.