United States Government Accountability Office

GAO

Report to Congressional Committees

October 2009

INFORMATION SECURITY

NASA Needs to Remedy Vulnerabilities in Key Networks

GAO-10-4

G A O
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-10-4, a report to congressional committees

Why GAO Did This Study

The National Aeronautics and Space Administration (NASA) relies extensively on information systems and networks to pioneer space exploration, scientific discovery, and aeronautics research. Many of these systems and networks are interconnected through the Internet, and may be targeted by evolving and growing cyber threats from a variety of sources.

GAO was directed to (1) determine whether NASA has implemented appropriate controls to protect the confidentiality, integrity, and availability of the information and systems used to support NASA's mission directorates and (2) assess NASA's vulnerabilities in the context of prior incidents and corrective actions. To do this, GAO examined network and system controls in place at three centers; analyzed agency information security policies, plans, and reports; and interviewed agency officials.

What GAO Recommends

GAO recommends that the NASA Administrator take steps to mitigate control vulnerabilities and fully implement a comprehensive information security program. In commenting on a draft of this report, NASA concurred with GAO's recommendations and stated that it will continue to mitigate the information security weaknesses identified.

To view the full report, click on GAO-10-4.
For more information, contact Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov or Dr. Nabajyoti Barkakati, (202) 512-4499, barkakatin@gao.gov.

October 2009

INFORMATION SECURITY

NASA Needs to Remedy Vulnerabilities in Key Networks

What GAO Found

Although NASA has made important progress in implementing security controls and aspects of its information security program, it has not always implemented appropriate controls to sufficiently protect the confidentiality, integrity, and availability of the information and systems supporting its mission directorates. Specifically, NASA did not consistently implement effective controls to prevent, limit, and detect unauthorized access to its networks and systems. For example, it did not always sufficiently (1) identify and authenticate users, (2) restrict user access to systems, (3) encrypt network services and data, (4) protect network boundaries, (5) audit and monitor computer-related events, and (6) physically protect its information technology resources. In addition, weaknesses existed in other controls to appropriately segregate incompatible duties and manage system configurations and implement patches. A key reason for these weaknesses is that NASA has not yet fully implemented key activities of its information security program to ensure that controls are appropriately designed and operating effectively. Specifically, it has not always (1) fully assessed information security risks; (2) fully developed and documented security policies and procedures; (3) included key information in security plans; (4) conducted comprehensive tests and evaluation of its information system controls; (5) tracked the status of plans to remedy known weaknesses; (6) planned for contingencies and disruptions in service; (7) maintained capabilities to detect, report, and respond to security incidents; and (8) incorporated important security requirements in its contract with the Jet Propulsion Laboratory.

Despite actions to address prior security incidents, NASA remains vulnerable to similar incidents. NASA networks and systems have been successfully targeted by cyber attacks. During fiscal years 2007 and 2008, NASA reported 1,120 security incidents that have resulted in the installation of malicious software on its systems and unauthorized access to sensitive information. To address these incidents, NASA established a Security Operations Center in 2008 to enhance prevention and provide early detection of security incidents and coordinate agency-level information related to its security posture. Nevertheless, the control vulnerabilities and program shortfalls, which GAO identified, collectively increase the risk of unauthorized access to NASA's sensitive information, as well as inadvertent or deliberate disruption of its system operations and services. They make it possible for intruders, as well as government and contractor employees, to bypass or disable computer access controls and undertake a wide variety of inappropriate or malicious acts. As a result, increased and unnecessary risk exists that sensitive information is subject to unauthorized disclosure, modification, and destruction and that mission operations could be disrupted.

Contents

Tables

Figures

Abbreviations

CIO	Chief Information Officer
DSN	Deep Space Network
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IONet	Internet Protocol Operational Network
IT	information technology
JPL	Jet Propulsion Laboratory
NASA	National Aeronautics and Space Administration
NISN	NASA Integrated Services Network Mission and Corporate Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
POA&M	plans of action and milestones
SOC	Security Operations Center
US-CERT	United States Computer Emergency Readiness Team

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 15, 2009

The Honorable John D. Rockefeller, IV
Chairman
The Honorable Kay Bailey Hutchison
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Bart Gordon
Chairman
The Honorable Ralph M. Hall
Ranking Member
Committee on Science and Technology
House of Representatives

The National Aeronautics and Space Administration's (NASA) mission is to pioneer the future in space exploration, scientific discovery, and aeronautics research. To carry out its critical mission and business operations, NASA depends on interconnected information systems. Many of these systems are interconnected through the public telecommunications infrastructure, including the Internet.

Government officials are concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations. For example, in February 2009, the Director of National Intelligence testified that foreign nations and criminals have targeted government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups have expressed a desire to use cyber attacks as a means to target the United States. To address such threats, NASA has implemented computer security controls that are intended to protect the confidentiality, integrity, and availability of its systems and information.

In response to a congressional mandate,[1] our objectives were to (1) assess the effectiveness of NASA's information security controls in protecting the confidentiality, integrity, and availability of its networks supporting

[1] National Aeronautics and Space Administration Authorization Act of 2008 Pub. L. No. 110-422, § 1001 (Oct. 15, 2008).

mission directorates and (2) assess the vulnerabilities identified during the audit in the context of NASA's prior security incidents and corrective actions. To accomplish these objectives, we examined computer security controls on networks at three centers supporting NASA's mission directorates to see whether resources and information were safeguarded and protected from unauthorized access. We conducted vulnerability assessments of network security with the knowledge of NASA officials, but we did not perform unannounced penetration testing during this review. We also reviewed and analyzed NASA's security policies, plans, and reports.

We performed this performance audit at NASA headquarters in Washington, D.C.; Goddard Space Flight Center in Greenbelt, Maryland; the Jet Propulsion Laboratory in Pasadena, California; the Marshall Space Flight Center in Huntsville, Alabama; and Ames Research Center in Moffett Field, California, from November 2008 to October 2009. See appendix I for further details of our objectives, scope, and methodology.

We conducted our audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Information security is a critical consideration for any organization reliant on information technology (IT) and especially important for government agencies, where maintaining the public's trust is essential. The dramatic expansion in computer interconnectivity, and the rapid increase in the use of the Internet, have changed the way our government, the nation, and much of the world communicate and conduct business. However, without proper safeguards, systems are unprotected from attempts by individuals and groups with malicious intent to intrude and use the access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. This concern is well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks to come.

Cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing. These threats can be unintentional or intentional, targeted or nontargeted, and can come from a variety of sources, such as foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization. Moreover, these groups and individuals have a variety of attack techniques at their disposal, and cyber exploitation activity has grown more sophisticated, more targeted, and more serious. As government, private sector, and personal activities continue to move to networked operations, as digital systems add ever more capabilities, as wireless systems become more ubiquitous, and as the design, manufacture, and service of IT have moved overseas, the threat will continue to grow. In the absence of robust security programs, federal agencies have experienced a wide range of incidents involving data loss or theft and computer intrusions, underscoring the need for improved security practices.

Recognizing the importance of securing federal agencies' information and systems, Congress enacted the Federal Information Security Management Act of 2002 (FISMA) to strengthen the security of information and information systems within federal agencies.[2] FISMA requires each agency to use a risk-based approach to develop, document, and implement an agencywide security program for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

NASA's Mission and Organization

The National Aeronautics and Space Act of 1958 (Space Act), as amended, established NASA as the civilian agency that exercises control over U.S. aeronautical and space activities and seeks and encourages the fullest commercial use of space.[3] NASA's mission is to pioneer the future of space exploration, scientific discovery, and aeronautics research. Its current and planned activities span a broad range of complex and technical endeavors, including deploying a global climate change research and monitoring

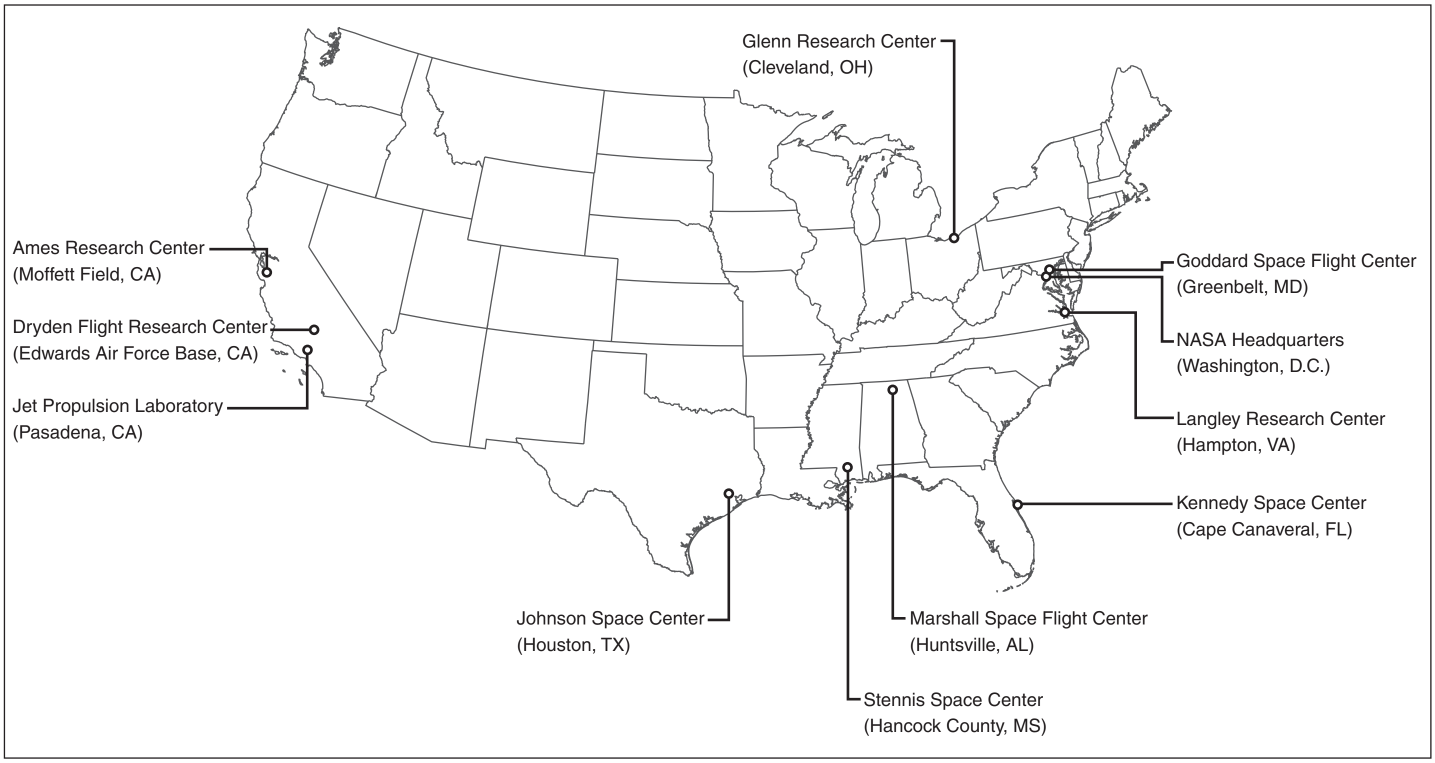
[2] FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

[3] Pub. L. No. 85-568, § 102 (b) and (c) (1958) (codified as amended at 42 U.S.C. § 2451 (b), (c), and (d)). The Department of Defense retains the activities peculiar to or primarily associated with the development of weapons systems, military operations, or the defense of the United States. 42 U.S.C. § 2451 (c).

system, returning Americans to the Moon and exploring other destinations, flying the Space Shuttle to complete the International Space Station, and developing new space transportation systems.

NASA is composed of a headquarters office in Washington, D.C., nine centers located around the country, and the Jet Propulsion Laboratory (JPL), which is a Federally Funded Research and Development Center[4] under a contract with the California Institute of Technology (see fig. 1).

Figure 1: NASA Headquarters, Centers, and the Jet Propulsion Laboratory


Glenn Research Center (Cleveland, OH)
Ames Research Center (Moffett Field, CA)
Dryden Flight Research Center (Edwards Air Force Base, CA)
Jet Propulsion Laboratory (Pasadena, CA)
Goddard Space Flight Center (Greenbelt, MD)
NASA Headquarters (Washington, D.C.)
Langley Research Center (Hampton, VA)
Kennedy Space Center (Cape Canaveral, FL)
Johnson Space Center (Houston, TX)
Marshall Space Flight Center (Huntsville, AL)
Stennis Space Center (Hancock County, MS)

Sources: NASA (data), Map Resources (map).

Headquarters

[4] Federally Funded Research and Development Centers meet some special long-term research or development needs of the government and are operated, managed, and/or administered by either a university or consortium of universities, other not-for-profit or nonprofit organizations, or an industrial firm, as an autonomous organization or as an identifiable separate operating unit of a parent organization.

Headquarters is responsible for providing the agency's strategic direction, top-level requirements, schedules, budgets, and oversight of its mission. The NASA Administrator is responsible for leading the agency and is accountable for all aspects of its mission, including establishing and articulating its vision and strategic priorities and ensuring successful implementation of supporting policies, programs, and performance assessments. In this regard, the Office of the Administrator has overall responsibility for overseeing the activities and functions of the agency's mission and mission support directorates and centers.

NASA Headquarters has the following four mission directorates that define the agency's major lines of business or core mission segments:

- *Aeronautics Research* pursues long-term, innovative, and cutting-edge research that develops tools, concepts, and technologies to enable a safer, more flexible, environmentally friendly, and more efficient national air transportation system. It also supports the agency's human and robotic reentry vehicle research.

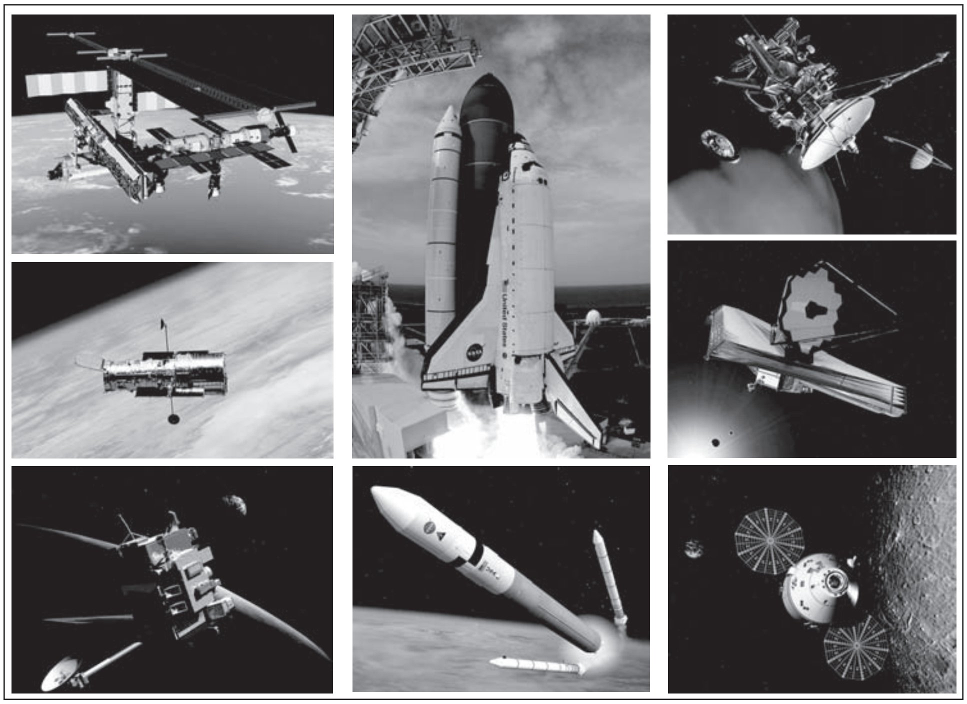
- *Exploration Systems* is leading the effort to develop capabilities for sustained and affordable human and robotic missions. The directorate is focused on developing the agency's next generation of human exploration spacecraft designed to carry crew and cargo to low Earth orbit and beyond, and partnering with industry and expanding the commercial technology sector. The directorate's responsibilities include operating the Lunar Reconnaissance Orbiter, Ares V Cargo Launch Vehicle, and Orion Crew Exploration Vehicle.

- *Science* carries out the scientific exploration of Earth and space to expand the frontiers of earth science, heliophysics, planetary science, and astrophysics. Through a variety of robotic observatory and explorer craft, and through sponsored research, the directorate provides virtual human access to the farthest reaches of space and time, as well as practical information about changes on Earth. The directorate's responsibilities include operating the Cassini orbiter, Hubble Space Telescope, and James Webb Space Telescope.

- *Space Operations* provides mission critical space exploration services to both NASA customers and to other partners within the United States and throughout the world. The directorate's responsibilities include flying the Space Shuttle to assemble the International Space Station, operating it after assembly is completed, and ensuring the health and safety of astronauts.

Each of the agency's four directorates is responsible and accountable for mission safety and success for the programs and projects assigned to it. Figure 2 contains images and artist renderings of some of the spacecraft that are deployed or in development that support the agency's programs and projects.

Figure 2: Examples of NASA Programs and Projects



Source: NASA.

Left to right: row 1, International Space Station, Space Shuttle, and Cassini orbiter; row 2, Hubble Space Telescope and James Webb Space Telescope; row 3, Lunar Reconnaissance Orbiter, Ares V Cargo Launch Vehicle, and Orion Crew Exploration Vehicle.

NASA headquarters also consists of mission support offices and other offices that advise the administrator and carry out the common or shared services that support core mission segments. These support offices include the Office of Chief Safety and Mission Assurance, Office of Security and Program Protection, Office of the Chief Financial Officer, Office of the Chief Information Officer, Office of the Inspector General, and Office of Institutions and Management. See appendix II for the agency's organization chart.

NASA Centers

Centers are responsible for executing the agency programs and projects. Each center has a director who reports to an Associate Administrator in the Office of the Administrator. A key institutional role of center directors is that of service across mission directorate needs and determining how best to support the various programs and projects hosted at a given center. Specific responsibilities include (1) providing resources and managing center operations; (2) ensuring that statutory, regulatory, fiduciary, and NASA requirements are met; and (3) establishing and maintaining the staff and their competency.

Jet Propulsion Laboratory

JPL is a Federally Funded Research and Development Center that is operated by the California Institute of Technology using government-owned equipment. The California Institute of Technology is under a contract with NASA that is renegotiated every 5 years. JPL develops and maintains technical and managerial competencies specified in the contract in support of NASA's programs and projects including (1) exploring the solar system to fully understand its formation and evolution, (2) establishing continuous permanent robotic presence on Mars to discover its history and habitability, and (3) conducting communications and navigation for deep space missions.

Headquarters, centers, and JPL support multiple mission directorates by taking on management responsibility and contributing to their programs and projects. See appendix III for a description of the missions of the individual centers and JPL. Table 1 identifies the mission directorates supported by each of these entities.

Table 1: Current Support of Mission Directorates by NASA Headquarters, Centers, and JPL

	Aeronautics Research	Exploration Systems	Science	Space Operations
Headquarters	X	X	X	X
Ames Research Center	X	X	X	
Dryden Flight Research Center	X	X	X	X
Glenn Research Center	X	X	X	X
Goddard Space Flight Center		X	X	X
Johnson Space Center		X	X	X
Kennedy Space Center		X	X	X
Langley Research Center	X	X	X	

	Aeronautics Research	Exploration Systems	Science	Space Operations
Marshall Space Flight Center		X	X	X
Stennis Space Center		X	X	X
Jet Propulsion Laboratory		X	X	X

Source: GAO analysis based on NASA data.

In fiscal year 2009, NASA had a budget of $17.78 billion and employed approximately 18,000 civil service employees and utilized approximately 30,000 contractor employees. NASA's budget request for fiscal year 2010 is $18.686 billion, which is roughly a 5 percent increase from fiscal year 2009. The agency's IT budget in fiscal year 2009 was $1.6 billion, of which $15 million was dedicated to IT security.

NASA Partners with a Variety of Organizations

The Space Act authorizes and encourages NASA to enter into partnerships that help fulfill its mission. Thus, the agency engages in strategic partnerships with other federal agencies, and a wide variety of academic, private sector, and international organizations to leverage their unique capabilities. For example, the agency partners with (1) the space agencies of Canada, Japan, and Russia as well as European Space Agency country members Belgium, Denmark, France, Germany, Italy, Netherlands, Norway, Spain, Sweden, and the United Kingdom; (2) federal agencies such as the Federal Aviation Administration, the Department of Energy, the National Oceanic and Atmospheric Administration, and the U.S. Air Force, Army, and Navy; (3) institutes, organizations, and universities in India, Finland, France, Latin America, New Zealand, the United Kingdom, and the United States; and (4) corporations such as Boeing and Lockheed Martin.

Key Networks Supporting NASA's Mission Directorates

NASA depends on a number of key computer systems and communication networks to conduct its work. These networks traverse the Earth and beyond providing critical two-way communication links between Earth and spacecraft; connections between NASA centers and partners, scientists, and the public; and administrative applications and functions. Table 2 lists several of the key networks supporting the agency.

Table 2: Examples of Key Networks Supporting NASA's Mission Directorates

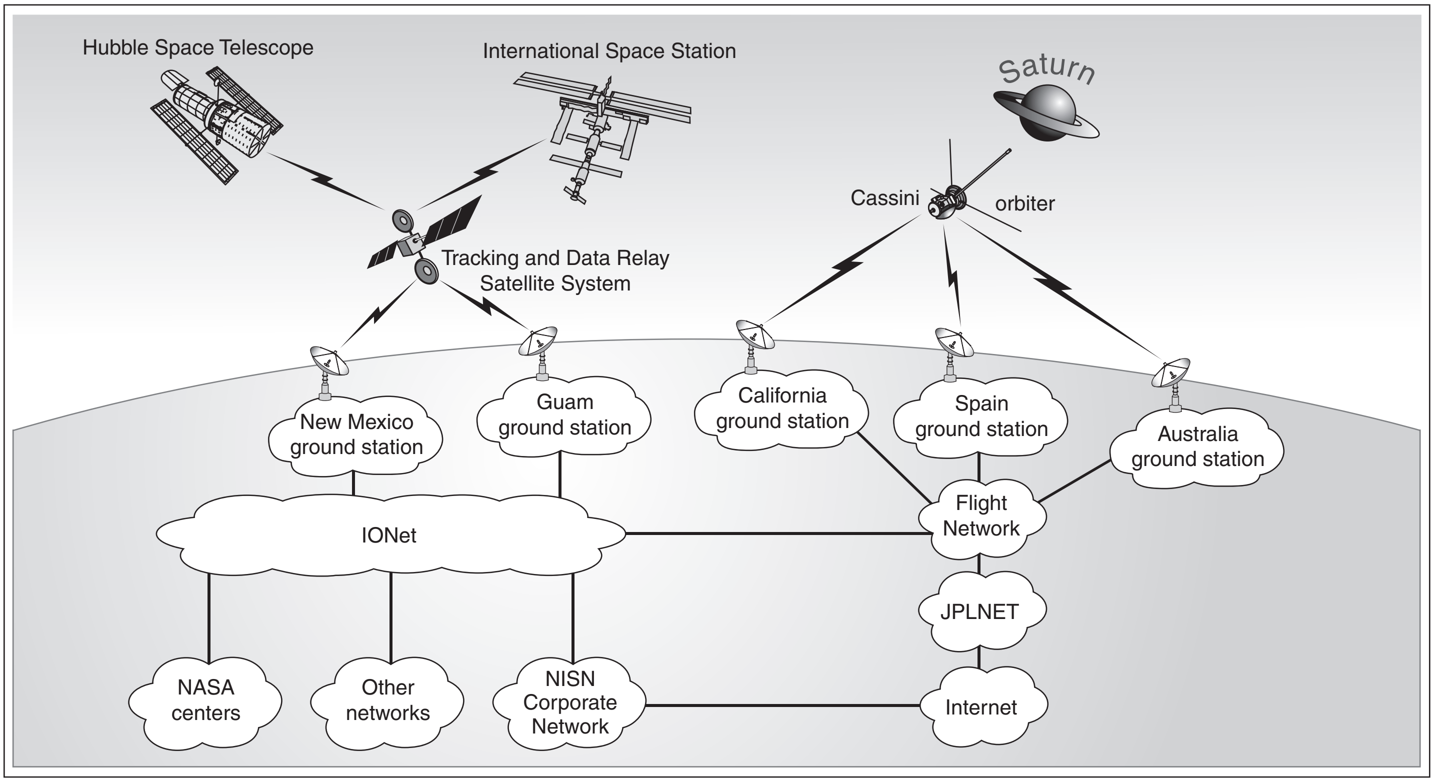
Network	Managing entity	Summary
Enhanced Huntsville Operations Support Center System	Marshall Space Flight Center	The ground system responsible for integrated operational payload flight control and planning for the International Space Station.
Flight Network	Jet Propulsion Laboratory	Includes (1) the Deep Space Network (DSN), which supports NASA's deep space missions and provides critical communications and tracking for multiple spacecraft including Cassini. The Flight Network consists of radio antennae strategically located at communication complexes in California, Spain, and Australia to ensure that as the Earth turns, most spacecraft will have one of these complexes facing them; (2) services and tools for conducting mission operations; (3) infrastructure devices; (4) a Domain Name Server; and (5) e-mail.
Integrated Collaborative Environment	Marshall Space Flight Center	A document management and life cycle management application at Marshall used to manage drawings and documents and to automate engineering processes for the Constellation Program, which includes the Ares V Crew Launch Vehicle and Orion projects.
Internet Protocol Operational Network (IONet)	Goddard Space Flight Center	A NASA-wide network that supports mission-critical spacecraft and science operations such as the Hubble Space Telescope and the Space Shuttle. It is also known as the NASA Integrated Services Network Mission Network (NISN).
JPLNET	Jet Propulsion Laboratory	JPL's administrative network that provides connectivity to its resources and hosts, the Internet, and NASA networks. JPLNET is not part of the JPL Flight Network.
NASA Integrated Services Network Mission and Corporate Network (NISN)	Goddard Space Flight Center/Marshall Space Flight Center	Comprised of a mission network segment managed by Goddard and a corporate network segment managed by Marshall. The mission network segment (also known as the Internet Protocol Operational Network) provides telecommunications systems and services for mission control, science data handling, and program administration. Its customer base includes all agency centers and headquarters, the DSN, most flight mission programs, contractors, international partners, academia, and government agencies.
NASA Operational Messaging and Directory Service	Marshall Space Flight Center	The agency's mission support e-mail system. Many parts of NASA have migrated to this system, and it is intended to be the corporate centralized e-mail solution for nonflight activities.

Source: GAO analysis based on NASA data.

Transmission of Satellite Data to Networks

Networks such as the DSN and the IONet send data to and receive data from spacecraft via satellite relays and ground antennae. Satellite telescopes accumulate status data such as the satellite's position and health, and science data such as images and measurements of the celestial object being studied. Data are stored onboard the satellite and transmitted to Earth in batches via satellite relays and ground antennae. For example, figure 3 illustrates how several of these networks are connected and communicate with spacecrafts, such as the Hubble Space Telescope, the International Space Station, and the Cassini orbiter.[5]

Figure 3: Simplified Illustration of Key Networks Supporting NASA Programs and Projects



Source: GAO analysis of agency data.

As shown above, the Cassini orbiter sends data directly to the ground station antennae at the communication complexes in Australia, California, and Spain. The Hubble Space Telescope and the International Space Station send data to ground station antennae via the Tracking and Data

[5] Figure 3 is neither intended to be a comprehensive illustration of the key mission network infrastructure at NASA, nor does it include protective elements such as firewalls and routers that are used to segregate networks. In addition, the drawing is purposely simplified and does not describe in detail the numerous networks at each center. Table 2 includes examples of other networks at Goddard, JPL, and Marshall. In figure 3, "other networks" include those of other federal agencies and NASA partners.

Relay Satellite System[6] to ground stations in New Mexico and Guam. Data received from spacecraft are stored at antenna facilities until they are distributed to the appropriate locations through ground communications such as IONet. When data are sent to spacecraft these pathways are reversed.

Information and Information Systems Supporting NASA Need Protection

Imperative to mission success is the protection of information and information systems supporting NASA. One of the agency's most valuable assets is the technical and scientific knowledge and information generated by NASA's research, science, engineering, technology, and exploration initiatives. The agency relies on computer networks and systems to collect, access, or process a significant amount of data that requires protection, including data considered mission-critical, proprietary, and/or sensitive but unclassified information. For example,

- the agencywide system controlling physical access to NASA facilities stores personally identifiable information such as fingerprints, Social Security numbers, and pay grades.
- an application for storing and sharing data such as computer-aided design and electrical drawings, and engineering documentation for Ares launch vehicles is being used by 7 agency data centers at 11 locations.

Accordingly, effective information security controls are essential to ensuring that sensitive information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure or manipulation, and destruction. The compromise or loss of such information could cause harm to a person's privacy or welfare, adversely impact economic or industrial institutions, compromise programs or operations essential to the safeguarding of our national interests, and weaken the strategic technological advantage of the United States.

NASA's Information Security Program

FISMA requires each federal agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by other

[6] The Tracking and Data Relay Satellite System consists of several satellites in geostationary orbits around the Earth.

agencies, contractors, or other sources. As described in table 3, NASA has designated certain senior managers at headquarters and its centers to fill the key roles in information security designated by FISMA and agency policy.

Table 3: Key NASA Information Security Responsibilities

NASA headquarters officials	Key responsibilities
NASA Administrator	Responsible for implementing a comprehensive and effective security program for the protection of people, property, and information associated with the NASA mission. The administrator must also ensure that the agency is in compliance with information security standards and guidelines.
NASA Chief Information Officer (CIO)	Responsible for the NASA-wide IT security program and has the management oversight responsibilities for ensuring the confidentiality, integrity, and availability of IT resources. The CIO's responsibilities are also met by (1) establishing policies and requirements necessary to comply with FISMA and ensure that NASA information and information systems are protected; (2) working with the mission directorates, support offices, centers, and program managers to reallocate funds to ensure that NASA complies with FISMA and the Office of Management and Budget (OMB) directives; and (3) reporting to NASA management and OMB on the status of the agency's IT Security Program.
NASA Deputy Chief Information Officer (CIO) for IT	Serves as the Senior Agency Information Security Officer and is responsible for implementing the IT security program of NASA; managing, coordinating, and maintaining the overall direction and structure of the NASA IT Security Program; and establishing standard operating procedures to ensure consistency of IT security objectives and solutions.
Assistant Administrator for the Office of Security and Program Protection	Responsible for all aspects of classified national security information matters, including establishing the certification and accreditation policies, procedures, and guidance for all classified IT systems operations. The Office of Security and Program Protection Assistant Administrator's responsibilities include coordinating with the Senior Agency Information Security Officer in the issuance of IT security alerts regarding potential threats and exploits that could affect NASA IT resources and networks.
NASA IT Security Officer	Responsible for ensuring the effectiveness of NASA IT security projects crossing agency centers and overseeing the NASA IT Security Awareness and Training Program.
Manager, Competency Center for IT Security	The NASA CIO's authorized organization to provide agencywide IT security leadership. The Competency Center for IT Security Manager is responsible for involving mission directorates, centers, and other stakeholders to ensure the timely introduction of new agency standards and services and for engaging center personnel in the definition and implementation of standards, guidelines, and services.
Center officials	
Center Director	Responsible for protecting the center's missions and programs, advocating support for IT security requirements, and providing the resources necessary to implement IT security requirements.
Center Chief Information Officer (CIO)	Responsible for providing sufficient resources to ensure compliance with agencywide IT security requirements, managing the center's network infrastructure to protect information system owners and to control unauthorized internet protocol addresses, and establishing an IT security incident response capability.

NASA headquarters officials	Key responsibilities
Center IT Security Manager	Responsible for implementing the Center IT Security Program, developing centerwide IT security policies and guidance, and maintaining an incident response capability. The IT Security Manager also ensures that center system security plans are compliant with guidance from the Senior Agency Information Security Officer and reports the center's IT security metrics status to center and agency management.
System-specific officials	
Information system owner	Responsible for the successful operation and protection of the system and its information. These individuals are usually civil service personnel acting as program, project, and functional managers but can be support service contractors or partners under agreements with NASA. Information system owners oversee the IT security of the systems or applications that are operated and managed through a support service contract, grant, or agreement. For government-owned, contractor-operated facilities such as JPL, a noncivil-service individual, at an equivalent civil service management level, may serve as the on-duty line manager.
Information owner	Responsible for the confidentiality, integrity, and availability of information. Although information owners may have their information processed by another organization, support service contractor, or partner, they are ultimately responsible for understanding any risk that another manager has accepted for the system processing their information.
Organization Computer Security Official	Responsible for a particular organization's IT security program. The Organization Computer Security Official serves as the critical communication link to and from that organization and its programs for all IT security matters. Specific responsibilities include reporting the status of the organization's IT security posture and suspected and actual IT security incidents to the Center IT Security Manager.
Information System Security Official	The principal staff advisor to the information system owner on all matters involving the IT security of the information system, including physical and personnel security, incident handling, and security training and education. The Information System Security Official plays an active role in developing and updating information system security plans and ensuring effective and timely reporting of all incidents and suspected incidents in accordance with center procedures.
System administrator	NASA civil service and support service contract system administrators are the managers and technicians who design and operate IT resources for their respective centers. They usually have privileged access to NASA information resources. Specific responsibilities include ensuring that security controls described in system security plans are properly implemented and following the center's incident response procedures.

Source: GAO analysis of NASA data.

Control Weaknesses Jeopardize NASA Systems and Networks

Although NASA had implemented many information security controls to protect networks supporting its missions, weaknesses existed in several critical areas. Specifically, the centers did not consistently implement effective electronic access controls, including user accounts and passwords, access rights and permissions, encryption of sensitive data, protection of information system boundaries, audit and monitoring of security-relevant events, and physical security to prevent, limit, and detect access to their networks and systems. In addition, weaknesses in other information system controls, including managing system configurations and patching sensitive systems, further increase the risk to the information and systems that support NASA's missions. A key reason for these weaknesses was that NASA had not yet fully implemented key elements of its information security program. As a result, highly sensitive personal, scientific, and other data were at an increased risk of unauthorized use, modification, or disclosure.

NASA Did Not Sufficiently Control Access to Information Resources

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Inadequate access controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service. Access controls include those related to (1) user identification and authentication, (2) user access authorizations, (3) cryptography, (4) boundary protection, (5) audit and monitoring, and (6) physical security. Weaknesses in each of these areas existed across the NASA environment.

Controls for Identifying and Authenticating Users Were Not Effectively Enforced

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system is able to distinguish one user from another—a process called identification. The system must also establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. The combination of identification and authentication—such as user account/password combinations—provides the basis for establishing individual accountability and for controlling access to the system. National Institute of Standards and Technology (NIST) states that (1) information systems should uniquely identify and authenticate users (or processes on behalf of users), (2) passwords should be implemented that are sufficiently complex to slow down attackers, (3) information systems should protect passwords from unauthorized disclosure and modification when stored and transmitted, and (4) passwords should be encrypted to ensure that the computations used in a dictionary or password cracking attack against a stolen password file cannot be used against similar password files.

NASA did not adequately identify and authenticate users in systems and networks supporting mission directorates. For example, NASA did not configure certain systems and networks at two centers to have complex passwords. Specifically, these systems and networks did not always require users to create long passwords. In addition, users did not need passwords to access certain network devices. Furthermore, encrypted password and network configuration files were not adequately protected, and passwords were not encrypted. As a result, increased risk exists that a malicious individual could guess or otherwise obtain user identification and passwords to gain network access to NASA systems and sensitive data.

User Access to NASA Systems Was Not Always Sufficiently Restricted

Authorization is the process of granting or denying access rights and privileges to a protected resource, such as a network, system, application, function, or file. A key component of granting or denying access rights is the concept of “least privilege.” Least privilege is a basic principle for securing computer resources and data that means that users are granted only those access rights and permissions that they need to perform their official duties. To restrict legitimate users’ access to only those programs and files that they need in order to do their work, organizations establish access rights and permissions. “User rights” are allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that are associated with a particular file or directory, regulating which users can access it—and the extent of that access. To avoid unintentionally giving users unnecessary access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions.

However, all three NASA centers we reviewed did not always sufficiently restrict system access and privileges to only those users that needed access to perform their assigned duties. For example, the centers did not always restrict access to sensitive files and control unnecessary remote access. In addition, NASA centers allowed shared accounts and group user IDs and did not restrict excessive user privileges. Furthermore, NASA centers did not effectively limit access to key network devices through access control lists. As a result, increased risk exists that users could gain inappropriate access to computer resources, circumvent security controls, and deliberately or inadvertently read, modify, or delete critical mission information.

NASA Implemented Encryption Controls but Did Not Always Encrypt Network Services and Sensitive Data

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic element of cryptography is encryption. Encryption can be used to provide basic data confidentiality and integrity by transforming plain text into ciphertext using a special value known as a key and a mathematical process known as an algorithm.[7] The National Security Agency (NSA) recommends encrypting network services. If encryption is not used, sensitive information such as user ID and password combinations are susceptible to electronic eavesdropping by devices on the network when they are transmitted. In addition, the OMB has recommended that all federal agencies encrypt all data on mobile devices like laptops, unless the data has been determined to be nonsensitive.

Although NASA has implemented cryptography, it was not always sufficient or used in transmitting sensitive information. For example, NASA centers did not always employ a robust encryption algorithm that complied with federal standards to encrypt sensitive information. The three centers we reviewed neither used encryption to protect certain network management connections, nor did they require encryption for authentication to certain internal services. Instead, the centers used unencrypted protocols to manage network devices, such as routers and switches. In addition, NASA had not installed full-disk encryption on its laptops at all three centers. As a result, sensitive data transmitted through the unclassified network or stored on laptop computers were at an increased risk of being compromised.

Although NASA Segregated Sensitive Networks, System Boundary Protection Was Not Always Adequate

Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from network connected devices. Unnecessary connectivity to an organization's network increases not only the number of access paths that must be managed and the complexity of the task, but the risk of unauthorized access in a shared environment. NIST guidance states that firewalls[8] should be configured to provide adequate protection for the organization's networks and that the transmitted information between interconnected systems should be controlled and regulated.

Although NASA had employed controls to segregate sensitive areas of its networks and protect them from intrusion, it did not always adequately control the logical and physical boundaries protecting its information and systems. For example, NASA centers did not adequately protect their

[7] A cryptographic algorithm and key are used to apply cryptographic protection to data (e.g., encrypt the data or generate a digital signature) and to remove or check the protection (e.g., decrypt the encrypted data or verify the digital signature).

[8] A firewall is a hardware or software component that protects computers or networks from attacks by blocking network traffic.

workstations and laptops from intrusions through the use of host-based firewalls. Furthermore, firewalls at the centers did not provide adequate protection for the organization’s networks, since they could be bypassed. In addition, the three centers had an e-mail server that allowed spoofed e-mail messages and potentially harmful attachments to be delivered to NASA. As a result, the hosts on these system networks were at increased risk of compromise or disruption from the other lower security networks.

Although NASA Monitored Its Networks, Monitoring Was Not Always Comprehensive

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine who has taken actions on the system, what these actions were, and when they were taken. According to NIST, when performing vulnerability scans, greater emphasis should be placed upon systems that are accessible from the Internet (e.g., Web and e-mail servers); systems that house important or sensitive applications or data (e.g., databases); or network infrastructure components (e.g., routers, switches, and firewalls). In addition, according to commercial vendors, running scanning software in an authenticated mode allows the software to detect additional vulnerabilities. NIST also states that the use of secure software development techniques, including source code review, is essential to preventing a number of vulnerabilities from being introduced into items such as a Web service. NASA requires that audit trails be implemented on NASA IT systems.

Although NASA regularly monitored its unclassified network for security vulnerabilities, the monitoring was not always comprehensive. For example, none of the three centers we reviewed conducted vulnerability scans for such sensitive applications as databases. In addition, the centers did not conduct source code reviews. Furthermore, not all segments and protocols on center networks were effectively monitored by intrusion detection systems. Moreover, NASA did not always configure several database systems to enable auditing and monitoring of security-relevant events and did not adequately perform logging of authentication, authorization, and accounting activities. As a result, NASA may not detect certain vulnerabilities or unauthorized activities, leaving the network at increased risk of compromise or disruption. Until NASA establishes detailed audit logs for its systems at these facilities or compensating controls in cases where such logs are not feasible, it risks being unable to determine if malicious incidents are occurring and, after an event occurs, being unable to determine who or what caused the incident.

Although NASA Had Various Physical Security Protections in Place, Weaknesses Existed

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted in order to ensure that it continues to be appropriate. NASA policy requires that its facilities and buildings be provided the level of security commensurate with the level of risk as determined by a vulnerability risk assessment. In addition, NASA policy requires enhanced security measures for its mission essential infrastructure such as computing facilities and data centers, including access control systems, lighting, and vehicle barriers such as bollards or jersey barriers. NIST policy also requires that federal agencies implement physical security and environmental safety controls to protect IT systems and facilities, as well as employees and contractors. These controls include protections to prevent excessive heat and fires or unnecessary water damage.

NASA had various protections in place for its IT resources. It effectively secured many of its sensitive areas and computer equipment and takes other steps to provide physical security. For example, all three NASA centers issued electronic badges to help control access to many of their sensitive and restricted areas. The agency also maintains liaisons with law enforcement agencies to help ensure additional security backup is available if necessary and to facilitate the accurate flow of timely security information among appropriate government agencies.

However, NASA's computing facilities may be vulnerable to attack because of weaknesses in controls over physical access points, including designated entry and exit points to the facilities where information systems reside. NASA also neither enforced stringent physical access measures for, and authorizations to, areas within a facility, nor did it maintain and review at least annually a current list of personnel with access to all IT-intensive facilities and properly authenticate visitors to these facilities. In addition, we were only able to obtain evidence that risk assessments were performed for 11 of the 24 NASA buildings we visited, which contained significant and sensitive IT resources. NASA also did not fully implement enhanced security measures for its mission essential infrastructure such as computing facilities and data centers. To illustrate, retractable bollards that protect delivery doors, generators, and fuel tanks at the data and communication centers were not operable and were in the "open" retracted position. NASA also did not fully follow NIST safety and security guidance. In addition, a data center that houses a large concentration of sensitive IT equipment including the laboratory's supercomputer had "wet pipe"[9] automatic sprinkler protection. This type of protection presents risks of water leaks that could do considerable damage to the sensitive and expensive computer equipment in the event of a fire. In addition, this data center's critical cooling equipment and fans located at the rear of the facility were not separately enclosed and protected. Although the facility's perimeter is fenced, an unauthorized individual could scale the fence and damage or sabotage the cooling equipment.

Because areas containing sensitive IT and support equipment were not adequately protected, NASA has less assurance that computing resources are protected from inadvertent or deliberate misuse including sabotage, vandalism, theft, and destruction.

Weaknesses in Other Important Controls Increase Risk

In addition to access controls, other important controls should be in place to ensure the security and reliability of an organization's information. These controls include policies, procedures, and control techniques to (1) appropriately segregate incompatible duties and (2) manage system configurations and implement patches. Weaknesses in these areas could increase the risk of unauthorized use, disclosure, modification, or loss of NASA's mission sensitive information.

Incompatible Duties Were Not Always Segregated

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often segregation of incompatible duties is achieved by dividing responsibilities among two or more organizational groups. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed.

[9] Wet pipe equipment is filled with water up to the automatic sprinkler head detection device. In contrast, dry pipe equipment does not deliver water into the pipes until an emergency occurs. Other automatic fire protection equipment does not use water but rather contains elements that remove oxygen from the room to extinguish the fire.

NASA did not adequately segregate incompatible duties. For example, all network users at two centers we reviewed had administrative privileges to their local computer and could install unapproved software. Only system administrators should have these privileges. As a consequence, increased risk exists that users could perform unauthorized system activities without detection.

Although NASA Maintained System Configurations and Installed Patches, Shortcomings Existed

Patch management is a critical process that can help alleviate many of the challenges of securing computing systems.[10] As vulnerabilities in a system are discovered, attackers may attempt to exploit them, possibly causing significant damage. Malicious acts can range from defacing Web sites to taking control of entire systems, thereby being able to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other organizations' systems. After a vulnerability is validated, the software vendor may develop and test a patch or work-around to mitigate the vulnerability. Incident response groups and software vendors issue information updates on the vulnerability and the availability of patches.

Although NASA had implemented innovative techniques to maintain system configurations and install patches, shortcomings existed. For example, all three NASA centers had not applied a critical operating system patch or patches for a number of general third-party applications. As a result, NASA had limited assurance that all needed patches were applied to critical system resources, increasing the risk of exposing critical and sensitive unclassified data to unauthorized access. Furthermore, although the three centers had configured their e-mail systems to prevent many common cyber attacks, they were still vulnerable to attack because their systems allowed various file types as e-mail attachments. These files could be used to install malicious software onto an unsuspecting user's workstation, potentially compromising the network. As a result, increased risk exists that an attacker could exploit known vulnerabilities in these applications to execute malicious code and gain control of or compromise a system.

[10] GAO, *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO-04-706 (Washington, D.C.: June 2, 2004).

NASA Has Not Fully Implemented Its Information Security Program

A key reason for these weaknesses is that although NASA has made important progress in implementing the agency's information security program, it has not effectively or fully implemented an agencywide information security program. FISMA requires agencies to develop, document, and implement an information security program that, among other things, includes

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;
- policies and procedures that (1) are based on risk assessments, (2) cost effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- plans for providing adequate information security for networks, facilities, and systems;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in its information security policies, procedures, or practices;
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency; and
- procedures for detecting, reporting, and responding to security incidents.

In addition, FISMA states the agency information security program applies to the information and information systems provided or managed by contractors or other sources.

We identified a number of shortcomings in key program activities. For example, NASA had not always (1) fully assessed information security risks; (2) fully developed and documented security policies and procedures; (3) included key information in security plans; (4) conducted comprehensive tests and evaluation of its information system controls; (5) tracked the status of plans to remedy known weaknesses; (6) planned for contingencies and disruptions in service; (7) maintained capabilities to detect, report, and respond to security incidents; and (8) incorporated important security requirements in its contract with JPL. Until all key elements of its information security program are fully and consistently implemented, NASA will have limited assurance that new weaknesses will not emerge and that sensitive information and assets are adequately safeguarded from inadvertent or deliberate misuse, improper disclosure, or destruction.

Although NASA Has Developed Risk Assessments, They Were Not Always Adequately Performed at Key Facilities

A comprehensive risk assessment should be the starting point for developing or modifying an agency's security policies and security plans. Such assessments are important because they help to make certain that all threats and vulnerabilities are identified and considered, that the greatest risks are addressed, and that appropriate decisions are made regarding which risks to accept and which to mitigate through security controls. Appropriate risk assessment policies and procedures should be documented and based on the security categorizations described in FIPS Publication 199.[11] OMB directs federal agencies to consider risk when deciding what security controls to implement. OMB states that a risk-based approach is required to determine adequate security, and it encourages agencies to consider major risk factors, such as the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. Identifying and assessing physical security risks are also essential steps in determining what information security controls are required. NASA policy states that vulnerability risk assessments for buildings and facilities are to be performed at least every 3 years.

NASA had generally implemented procedures for assessing its security risks and conducted risk assessments for the five systems and networks we reviewed. It had also determined security categories for these systems and networks. In addition, NASA had developed an executive threat summary on cyber issues facing the agency. Also, NASA's Security Operations Center (SOC) regularly issued threat analysis reports and distributed them to offices within NASA responsible for security.

[11] National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS PUB) 199 (December 2003).

However, NASA had not fully assessed its risks. For example, it had not conducted a comprehensive agencywide risk assessment that included mission-related systems and applications. In addition, one center we reviewed did not prepare an overall network risk assessment that clearly articulated the known vulnerabilities identified in the security plans and waivers.[12] Furthermore, the waivers were not elevated or aggregated and documented into an overall risk management plan. NASA also could not demonstrate that it conducted vulnerability risk assessments for 13 of the 24 buildings we visited that contained significant and sensitive information resources. NASA staff stated that some of the 13 buildings may have had risk assessments performed in the past, but they could not provide copies of the assessments or evidence to support these assertions. As a result, NASA has limited assurance that computing resources are consistently and effectively protected from inadvertent or deliberate misuse including fraud or destruction.

Although NASA Developed Security Policies and Procedures, It Did Not Always Include Key Elements

Another key task in developing an effective information security program is to establish and implement risk-based policies, procedures, and technical standards that govern security over an agency's computing environment. If properly implemented, policies and procedures should help reduce the risk that could come from unauthorized access or disruption of services. Because security policies and procedures are the primary mechanisms through which management communicates views and requirements, it is important that these policies and procedures be established and documented. FISMA requires agencies to develop and implement policies and procedures to support an effective information security program. NIST also issued security standards and related guidance to help agencies implement security controls, including appropriate information security policies and procedures.

NASA developed and documented several information security policies and procedures. For example, NASA established standard operating processes that had been successful in producing a number of IT procedures relating to certification and accreditation. However, NASA had not always included all the necessary elements in its security policies and procedures, as illustrated by the following examples:

[12] The waivers process constitutes the mechanism by which to document decisions to exceed the institutionally provided requirements and protective measures or accept additional risks.

- The agency did not have a policy for malware incident handling and prevention.

- Although NASA defined some security roles, it did not define all necessary roles and responsibilities for incident response and detection. Presently the only formal role for managing incidents as defined by NASA policy is the Information Technology Security Manager. However, NASA policy did not clearly define roles and responsibilities for incident response within NASA, such as an intrusion analyst or incident response manager.

- NASA had not updated the policy for incident handling to reflect the current environment. Although NASA has developed policy directives pertaining to incident handling that all NASA centers are required to follow, these documents had not been updated to reflect the November 2008 establishment of the SOC.

- Physical and environmental policies for the protection of NASA assets were not adequately defined. NASA's policies do not adequately describe physical access controls such as authorizing, controlling, and monitoring physical access to sensitive locations. For example, regarding monitoring, the agency's policy does not clearly require that officials maintain and review at least annually a current list of personnel with access to all IT-intensive facilities. Additionally, NASA's policies did not provide clear and consistent guidance for developing and implementing environmental safety controls. For instance, the agency's policies and procedures lacked information on fire protection and emergency power shutoff. NASA IT and physical security policy staff acknowledged these shortcomings and stated that new policies are being or will be drafted during this calendar year and should be approved by NASA management around the end of calendar year 2010.

Until these policies are fully developed and documented across all agency centers, NASA has less assurance that computing resources are consistently and effectively protected from inadvertent or deliberate misuse, including fraud or destruction.

NASA Prepared Security Plans but Did Not Always Include All Key Information

An objective of system security planning is to improve the protection of IT resources. A system security plan provides a complete and up-to-date overview of the system's security requirements and describes the controls that are in place—or planned—to meet those requirements. OMB Circular A-130 specifies that agencies develop and implement system security plans for major applications and general support systems[13] and that these plans address policies and procedures for providing management, operational, and technical controls. NIST guidance states that these plans should be updated as system events trigger the need for revision in order to accurately reflect the most current state of the system. NIST guidance requires that all security plans be reviewed and, if appropriate, updated at least annually.

NASA generally prepared and documented security plans for the five systems and networks we reviewed. In addition, NASA has developed and mandated the use of the Risk Management System as the authoritative source for the creation and storage of system security plans and documentation. Most notably, JPL also employed a real-time Certification and Accreditation document repository system, which facilitates a more repeatable process and ensures consistency and correctness.

However, NASA did not always include key information in system security plans. For example, NASA did not always update one system security plan with the results from its network risk assessment and threat analysis. In addition, system interconnection security agreements were not always signed for all external connections. Specifically, a center did not have signed interconnection security agreements for any connections with its partners and stakeholders. Furthermore, interconnection security agreements for one network were still pending. Without a security plan that describes security requirements and specific threats as identified in the risk assessment, and without having signed interconnection security agreements, NASA networks remain vulnerable to threats.

NASA Conducted System Security Tests, but They Were Not Always Comprehensive

A key element of an information security program is to test and evaluate policies, procedures, and controls to determine whether they are effective and operating as intended. This type of oversight is a fundamental element of a security program because it demonstrates management's commitment to the program, reminds employees of their roles and responsibilities, and identifies areas of noncompliance and ineffectiveness. Analyzing the results of security reviews provides security specialists and business

[13] OMB Circular A-130, Appendix III, defines a major application as one that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. It defines a general support system as an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

managers with a means of identifying new problem areas, reassessing the appropriateness of existing controls (management, operational, technical), and identifying the need for new controls. FISMA requires that the frequency of tests and evaluations be based on risks and occur no less than annually.[14]

NASA commissioned penetration testing using a rotational audit approach that covered various NASA centers. The scope of the tests included internal and external network-based penetration testing, Web application testing against center-selected Web sites, war-driving to identify rogue and unprotected wireless access points, configuration testing on center workstations and networking devices, searches for publicly available sensitive data, and social engineering scenarios against help desk staff.

Although NASA conducted system security testing and evaluating on the five systems and networks we reviewed, the tests were not always comprehensive. For instance, NASA did not test all relevant security controls and did not identify certain weaknesses that we identified during our review. For example, our review revealed problems with a firewall that were not identified by a test, including the fact that the firewall can be bypassed. In addition, the network documentation highlighted managerial control issues, such as the lack of policy, but insufficient or limited attention was paid to testing weaknesses in operational and technical controls. As a result, NASA could be unaware of undetected vulnerabilities in its networks and systems and has reduced assurance that its controls are being effectively implemented.

Remedial Action Plans Were Not Always Tracked Effectively

Remedial action plans, also known as plans of action and milestones (POA&M), can help agencies identify and assess security weaknesses in information systems and set priorities and monitor progress in correcting them. NIST guidance states that each federal civilian agency must report all incidents and internally document remedial actions and their impact. In addition, NASA policy states that all master and subordinate IT system POA&Ms should be tracked and reported to the NASA CIO in a timely manner so that corrective actions can be taken.

Although NASA has developed and implemented a remedial action process, it did not always prepare remedial action plans for known control deficiencies or report the status of corrective actions in a centralized

[14] 44 U.S.C. § 3544 (b) (5).

remediation tracking system maintained by the NASA CIO.[15] For example, NASA did not develop POA&Ms to correct several weaknesses documented in one system's security assessment or to address remediation threats documented in its risk assessment. In addition, the NASA centers we reviewed did not always report remedial action plans and the status of corrective actions into the central Headquarters Risk Management System used for POA&Ms. Consequently, senior management officials were not always aware of control weaknesses that still remained outstanding. Without an effective remediation program, identified vulnerabilities may not be resolved in a timely manner, thereby allowing continuing opportunities for unauthorized individuals to exploit these weaknesses and gain access to sensitive information and systems.

NASA Did Not Always Adequately Plan for Contingencies

Contingency planning is a critical component of information protection. If normal operations are interrupted, network managers must be able to detect, mitigate, and recover from service disruptions while preserving access to vital information. Therefore, a contingency plan details emergency response, backup operations, and disaster recovery for information systems. It is important that these plans be clearly documented, communicated to potentially affected staff, and updated to reflect current operations. NIST also requires that all of an agency's systems have a contingency plan and that the plans address, at a minimum, identification and notification of key personnel, plan activation, system recovery, and system reconstitution. NASA guidance states that contingency plans should describe an alternate backup site in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site. The guidance also states that contingency plans should include contact information for disaster recovery personnel.

NASA had developed contingency plans for the five systems and networks we reviewed. However, shortcomings existed in several plans. Specifically, (1) NASA did not approve the contingency plans for one network and one system we reviewed; (2) it did not include contact information for disaster recovery personnel at a center, even though their roles and responsibilities for disaster recovery were described; (3) NASA did not describe an alternate backup site for a center in a geographic area outside of the

[15] The Deputy CIO also evaluated NASA's remedial action process in October 2007 and stated that, due to the fragmented organization, not every center reports to the CIO headquarters diligently on corrective action plans for reported vulnerabilities discovered in the security testing and evaluation.

primary site, and had not designated backup facilities for a network we reviewed; and (4) the contingency plan for a system we reviewed did not follow NASA's guidance on contingency planning, since it did not include review and approval signatures, information contact(s) and line of succession, and damage assessment procedures. As a result, NASA is at a greater risk for major service disruptions with respect to its important mission networks in the event of a disaster to the primary facility.

NASA Has Implemented Incident Detection and Handling Capabilities, but They Remain Limited

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they take steps to promptly detect and respond to them before significant damage is done. NIST offers the following guidance for establishing an effective computer security incident response capability. Organizations should create an incident response policy, and use it as the basis for incident response procedures, that defines which events are considered incidents, establishes the organizational structure for incident response, defines roles and responsibilities, and lists the requirements for reporting incidents, among other items. In addition, organizations should acquire the necessary tools and resources for incident handing, including communications, facilities, and the analysis of hardware and software.

NASA has established a computer security incident handling project to respond to incidents. As part of this project, NASA has implemented a SOC, within Ames Research Center, which is the central coordination point for NASA's incident handling program and for reporting of incidents to the United States Computer Emergency Readiness Team (US-CERT).[16] The SOC began operations in November 2008 and is expected to enhance prevention and provide early detection of security incidents and coordinate agency-level information related to NASA's IT security posture. The SOC has implemented an agency hotline for security incidents and a centralized incident management system for the coordination, tracking, and reporting of agency incidents. It is currently improving its infrastructure to support detection, notification, investigation, and response to incidents in a timely manner. In addition to the SOC, the three centers that we reviewed had their own teams of incident responders that addressed and tracked incidents at their centers.

[16] US-CERT is a component of the Department of Homeland Security and is responsible for analyzing and addressing cyber threats and vulnerabilities and disseminating cyber-threat warning information. Federal agencies, including NASA, are required to report security incidents to US-CERT.

However, NASA's capabilities to detect, report, and respond to security incidents remain limited. The following are examples:

- The agency is not using a consistent definition of an incident. Responders at several centers stated they were following the NIST/US-CERT definition of an incident, which makes no distinction between an event and an incident. Although a center's standard operating procedure did not include a formal definition of a computer security incident, the center personnel stated that incidents are only those that are confirmed. However, a definition of what constitutes a "confirmed" incident was not provided.
- The organizational structure for incident response roles and responsibilities was outdated since it assigned central coordination and analysis of incidents to an organization that no longer existed. Although the SOC has developed an incident management plan, policies, and procedures for responding to incidents, they were in draft and had not been distributed to all the centers.
- Although two of the centers support mission related operations that operate 24x7, the two centers' incident response teams were not staffed around the clock.
- The business impacts of incidents were not adequately specified in NASA incident documentation. NASA incident documentation contains references to the fact that data subject to International Traffic in Arms Regulations[17] were stolen along with a laptop. However, the precise data that were lost were described only in very general terms so that the business impacts are not known. Moreover, although agency officials stated that conducting root cause analyses is required and part of the standard incident response workflow, there were many incidents for which a detailed post-incident analysis was not performed.

In addition, weaknesses in NASA's technical controls impact its incident handling and detection controls. For example, two centers we reviewed did not employ host-based firewalls on their workstations, laptops, or devices. In addition, one network had limited incident detection systems to detect malicious traffic coming from its internal and off-site connections. Moreover, another network had no internal incident

[17] 22 C.F.R. Subchapter M Parts 120-130. The International Traffic in Arms Regulations are promulgated by the U.S. Department of State under the Arms Export Control Act (22 U.S.C. 2778) for the control of the permanent and temporary export and the temporary import of defense articles and defense services.

detection system in place to monitor traffic, with the partial exception of network incident detection coverage of ingress/egress for it. Furthermore, one center had not adequately established and implemented tools and processes to ensure timely detection of security incidents.

As a result, there is a heightened risk that NASA may not be able to detect, contain, eradicate, or recover from incidents, and improve the incident handling process.

NASA Did Not Include Important Security Requirements in Its Contract

The agencywide information security program required by FISMA applies not only to information systems used or operated by an agency but also to information systems used or operated by a contractor of an agency or other agency on behalf of an agency. In addition, the Federal Acquisition Regulation (FAR) requires that federal agencies prescribe procedures for ensuring that agency planners on IT acquisitions comply with the IT security requirements of FISMA, OMB's implementing policies, including appendix III of OMB Circular A-130, and guidance and standards from NIST.[18] Appropriate policies and procedures should be developed, implemented, and monitored to ensure that the activities performed by external third parties are documented, agreed to, implemented, and monitored for compliance.

However, NASA did not adequately incorporate information security requirements in its contract with the JPL contractor. Although the contract for JPL specified adherence to certain NASA security policies,[19] it did not require the contractor to implement key elements of an information security program. For example, the following NASA and FISMA requirements are not specifically referenced in the JPL contract:

- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices performed with a frequency depending on risk, but not less than annually, and including testing of management, operational, and technical controls for every system.

[18] The FAR was established to codify uniform policies for acquisition of supplies and services by executive agencies. The FAR appears in the Code of Federal Regulations in Title 48. See 48 C.F.R. 7.103 (u).

[19] The actual contract language says "Documents referenced in the NASA policy 2810.1A are not applicable unless expressly incorporated in the Contract."

- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency.

- Procedures for detecting, reporting, and responding to security incidents.

- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

In addition, NASA did not incorporate provisions in the contract to allow it to perform effective oversight of the contractor's implementation of the security controls and program. For example, the JPL contract did not recognize the oversight roles of the NASA Administrator, the NASA CIO, the senior agency information security officer and other senior NASA managers as defined in NASA's policy.[20]

As a result, NASA faces a range of risks from contractors and other users with privileged access to NASA's systems, applications, and data since contractors that provide users with privileged access to agency/entity systems, applications, and data can introduce risks to their information and information systems.

Despite Actions to Address Security Incidents, NASA Remains Vulnerable

NASA has experienced numerous cyber attacks on its networks and systems in recent years. During fiscal years 2007 and 2008, NASA reported 1,120 security incidents to US-CERT in the following five US-CERT-defined categories:

- *Unauthorized access:* Gaining logical or physical access without permission to a federal agency's network, system, application, data, or other resource.

- *Denial of service:* Preventing or impairing the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of or participating in a denial of service attack.

[20] Chapter 2 of NASA Policy 2810.1A, the *NASA Information Security Policy Manual*, outlining the roles and responsibilities of senior management, IT Security System and Information owners, Center IT Security Supporting Functions, certification and accreditation roles, NASA Senior IT Security Management Working Relationships, etc. is specifically "not accepted" in the JPL contract.

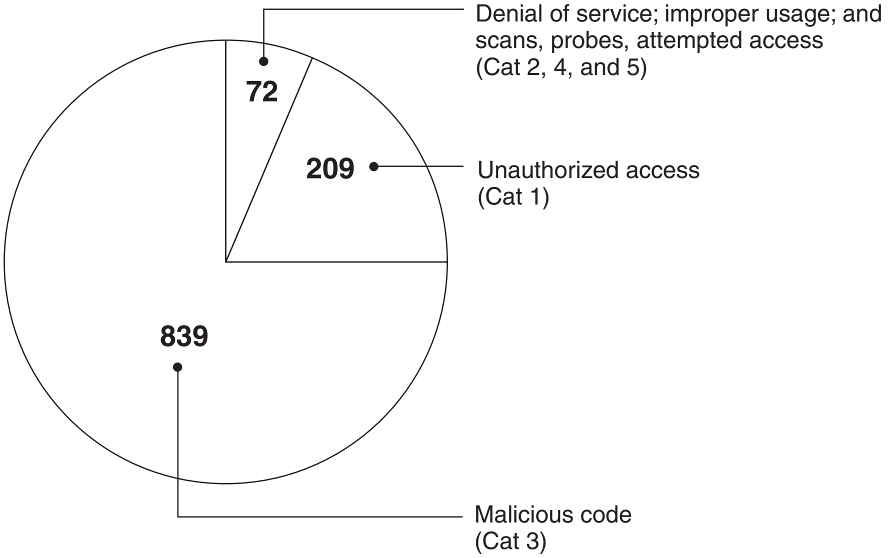
- *Malicious code:* Installing malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.

- *Improper usage:* Violating acceptable computing use policies.

- *Scans/probes/attempted access:* Accessing or identifying a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. This activity does not directly result in a compromise or denial of service.

As noted in figure 4, the two most prevalent types of incidents reported by NASA were malicious code[21] and unauthorized access.

Figure 4: Total Computer Security Incidents in Categories 1 through 5 Reported by NASA to US-CERT for Fiscal Years 2007-2008



Source: GAO analysis of US-CERT data.

[21] Malicious code is also known as malware and, according to NIST, has become the most significant external threat to most systems, causing widespread damage and disruption, and necessitating extensive recovery efforts within most organizations. Malware refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.

A NASA report stated that the number of malicious code attacks (839) was the highest experienced by any of the federal agencies, which accounted for over one-quarter of the total number of malicious code attacks directed at federal agencies during this period. According to an official at the US-CERT, NASA's high profile makes the agency an attractive target for hackers seeking recognition, or for nation-state sponsored cyber spying.

The impact of these and more recent incidents can be significant. The following examples are illustrative:

- In 2009, NASA reported incidents involving unauthorized access to sensitive data. For example, one center reported the theft of a laptop containing data subject to International Traffic in Arms Regulations. Stolen data included roughly 3,000 files of unencrypted International Traffic in Arms Regulations data with information for Hypersonic Wind Tunnel testing for the X-51 scramjet project and possibly personally identifiable information. Another center reported the theft of a laptop containing thermal models, review documentation, test plans, test reports, and requirements documents pertaining to NASA's Lunar Reconnaissance Orbiter and James Webb Space Telescope projects. The incident report does not indicate whether this lost data was unencrypted or encrypted or how the incident was resolved. Significantly, these were not isolated incidents since NASA reported 209 incidents of unauthorized access to US-CERT during fiscal years 2007 and 2008.

- One center was alerted by the NASA SOC in February 2009 about traffic associated with a Seneka Rootkit Bot.[22] In this case, NASA found that 82 NASA devices had been communicating with a malicious server since January 2009. A review of the data revealed that most of these devices were communicating with a server in the Ukraine. By March 2009, three centers were also infected with the bot attack.

- In October 2007, a total of 86 incidents related to the Zonebac Trojan[23] were reported by NASA centers. This particular form of malware is capable of disabling security software and downloading and running other

[22] "Bots" are infected machines under the control of persons other than the intended users that are used as proxies for attacks on other systems or for storage and distribution of pirated and other illicit content.

[23] Trojan horses are nonreplicating programs that appear to be benign but actually have a hidden malicious purpose. Some Trojan horses are intended to replace existing files, such as system and application executables, with malicious versions; others add another application to systems instead of overwriting existing files.

malicious software at the whim of the attacker. US-CERT reported in January 2008 on NASA's ongoing problems with Zonebac and other malware infestations and recommended that the agency employ consistent patching and user education practices to prevent such infections from occurring.

- In July 2008, NASA found several hosts infected with the Coreflood Trojan that is capable of frequently updating itself and stealing a large number of user credentials that can be used to log onto other machines within a domain. Investigation revealed that NASA computers were infected and communicating with a hostile command and control server.

These attacks can result in damage to applications, data, or operating systems; disclosure of sensitive information; propagation of malware; use of affected systems as bots; an unavailability of systems and services; and a waste of time, money, and labor.

In response to these and other attacks, NASA has enhanced its incident response capabilities and computer defensive capabilities at NASA's centers. For example, the three centers that we reviewed had their own teams of incident responders that addressed and tracked incidents at their centers. In addition, the SOC was established in 2008 to enhance prevention and provide early detection of security incidents and coordinate agency-level information related to NASA's security posture. The SOC has implemented an agency hotline for security incidents and an incident management system for the coordination and tracking of agency security incidents. It is currently improving its infrastructure to support detection, notification, investigation, and response to security incidents in a timely manner.

Despite actions to address security incidents, NASA remains vulnerable to similar incidents going forward. The control vulnerabilities and program shortfalls that we identified collectively increase the risk of unauthorized access to NASA's sensitive information, as well as inadvertent or deliberate disruption of its system operations and services. They make it possible for intruders, as well as government and contractor employees, to bypass or disable computer access controls and undertake a wide variety of inappropriate or malicious acts. As a result, increased and unnecessary risk exists that sensitive information will be subject to unauthorized disclosure, modification, and destruction and that mission operations could be disrupted.

Conclusions

Information security weaknesses at NASA impair the agency's ability to ensure the confidentiality, integrity, and availability of sensitive information. The systems supporting NASA's mission directorates at the three centers we reviewed have vulnerabilities in information security controls that place mission sensitive information, scientific, other data, and information systems at increased risk of compromise. A key reason for these vulnerabilities is that NASA has not yet fully implemented its information security program to ensure that controls are appropriately designed and operating effectively.

NASA's high profile and cutting edge technology makes the agency an attractive target for hackers seeking recognition, or for nation-state sponsored cyber spying. Thus, it is vital that attacks on NASA computer systems and networks are detected, resolved, and reported in a timely fashion and that the agency has effective security controls in place to minimize its vulnerability to such attacks. Despite actions to address previous security incidents, the control vulnerabilities and program shortfalls we identified indicate that NASA remains vulnerable to future incidents. These weaknesses could allow intruders, as well as government and contractor employees, to bypass or disable computer access controls and undertake a wide variety of inappropriate or malicious acts. Until NASA mitigates identified control vulnerabilities and fully implements its information security program, the agency will be at risk of unauthorized disclosure, modification, and destruction of its sensitive information and disruption of critical mission operations.

Recommendations for Executive Action

To assist NASA in improving the implementation of its agencywide information security program, we recommend that the NASA Administrator direct the NASA CIO to take the following eight actions:

- Develop and implement comprehensive and physical risk assessments that include mission-related systems and applications and known vulnerabilities identified in the security plans and waivers.

- Develop and fully implement security policies and procedures for malware, incident handling roles and responsibilities, and physical environmental protection.

- Include key information for system security plans such as information from risk assessments and signed system interconnection security agreements.

- Conduct sufficient or comprehensive security testing and evaluation of all relevant security controls including management, operational, and technical controls.
- Develop remedial action plans to address any deficiencies and ensure that master and subordinate IT system items are tracked and reported to the agency CIO in a timely manner so that corrective actions can be taken.
- Update contingency plans to include key information such as, contact information and approvals, and describe an alternate backup site in a geographic area that is unlikely to be negatively affected by the same disaster event.
- Implement an adequate incident detection program to include a consistent definition of an incident, incident roles and responsibilities, resources to operate the program, and business impacts of the incidents.
- Include all necessary security requirements in the JPL contract.

In a separate report with limited distribution, we are also making 179 recommendations to address the 129 weaknesses identified during this audit to enhance NASA's access controls.

Agency Comments and Our Evaluation

In providing written comments on a draft of this report (reprinted in app. IV), the NASA Deputy Administrator concurred with our recommendations and noted that many of the recommendations are currently being implemented as part of an ongoing strategic effort to improve information technology management and IT security program deficiencies. In addition, she stated that NASA will continue to mitigate the information security weaknesses identified in our report. The actions identified in the Deputy Administrator's response will, if effectively implemented, improve the agency's information security program.

We are sending copies to interested congressional committees, the Office of Management and Budget, the NASA Administrator, the NASA Inspector General and other interested parties. The report also is available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov or barkakatin@gao.gov. GAO staff who made major contributions to this report are listed in appendix V.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Nabajyoti Barkakati

Dr. Nabajyoti Barkakati
Chief Technologist

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) determine the effectiveness of the National Aeronautics and Space Administration's (NASA) information security controls in protecting the confidentiality, integrity, and availability of its networks supporting mission directorates and (2) assess the vulnerabilities identified during the audit in the context of NASA's prior security incidents and corrective actions.

To determine the effectiveness of security controls, we reviewed networks at three centers to gain an understanding of the overall network control environment, identified its interconnectivity and control points, and examined controls for NASA networks.

Using our *Federal Information System Controls Audit Manual*,[1] which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information, National Institute of Standards and Technology (NIST) standards and guidance, and NASA's policies, procedures, practices, and standards, we evaluated controls by

- developing an accurate understanding of the overall network architecture and examining configuration settings and access controls for routers, network management servers, switches, and firewalls;
- reviewing the complexity and expiration of password settings to determine if password management was enforced;
- analyzing users' system authorizations to determine whether they had more permissions than necessary to perform their assigned functions;
- observing methods for providing secure data transmissions across the network to determine whether sensitive data were being encrypted;
- observing whether system security software was logging successful system changes;
- observing physical access controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft;

[1] GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

- inspecting key servers and workstations to determine whether critical patches had been installed or were up-to-date; and
- examining access responsibilities to determine whether incompatible functions were segregated among different individuals.

Using the requirements identified by the Federal Information Security Management Act of 2002 (FISMA), which establishes key elements for an effective agencywide information security program, we evaluated five NASA systems and networks by

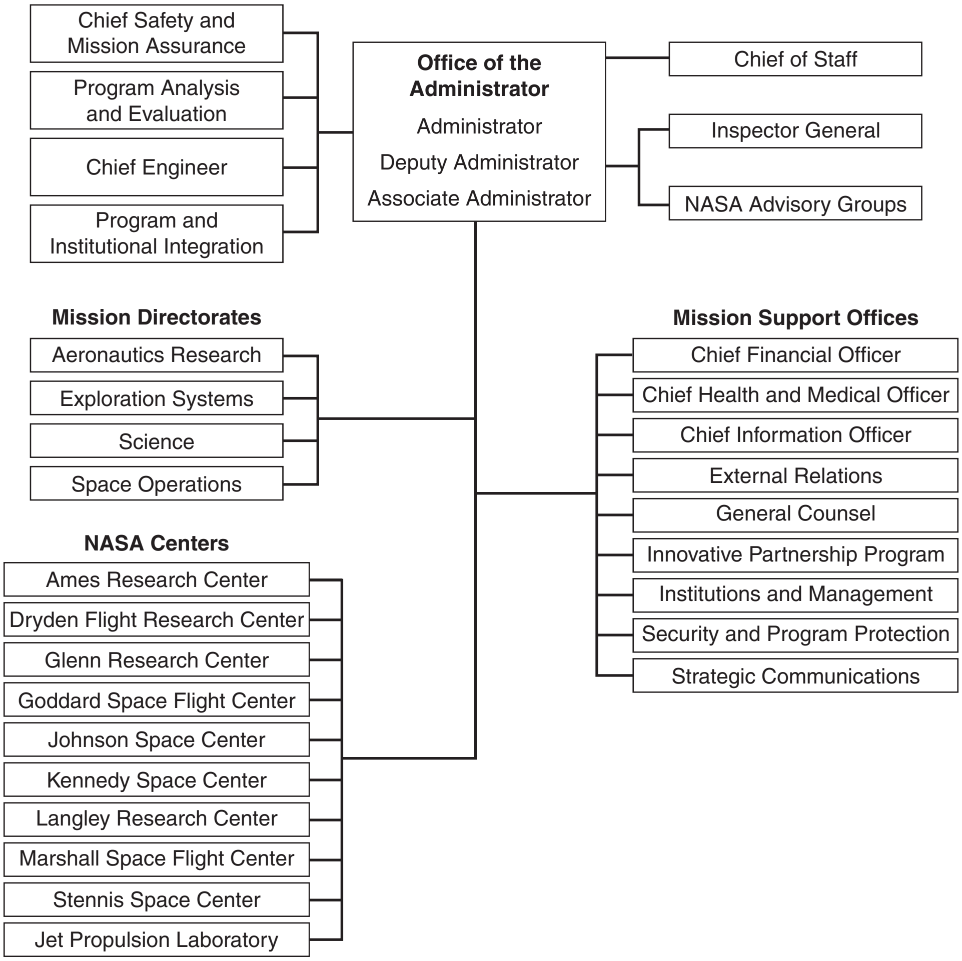
- analyzing NASA's policies, procedures, practices, standards, and resources to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems;
- reviewing NASA's risk assessment process and risk assessments to determine whether risks and threats were documented consistent with federal guidance;
- analyzing security plans to determine if management, operational, and technical controls were in place or planned and that security plans reflected the current environment;
- analyzing NASA's procedures and results for testing and evaluating security controls to determine whether management, operational, and technical controls were sufficiently tested at least annually and based on risk;
- examining remedial action plans to determine whether they addressed vulnerabilities identified in NASA's security testing and evaluations;
- examining contingency plans to determine whether those plans contained essential information, reflected the current environment, and had been tested to assure their sufficiency;
- reviewing incident detection and handling policies, procedures, and reports to determine the effectiveness of the incident handling program; and
- analyzing whether security requirements were implemented effectively by the contractor.

We also discussed with key security representatives and management officials whether information security controls were in place, adequately designed, and operating effectively.

To assess NASA's vulnerabilities in the context of prior incidents and corrective actions, we reviewed and analyzed United States Computer Emergency Readiness Team (US-CERT) data on NASA's reported incidents, examined NASA security incident reports in the last two fiscal years, inspected plans for corrective actions and the implementation of the Security Operations Center, and interviewed NASA officials on how NASA corrected identified vulnerabilities.

We performed our audit at NASA headquarters in Washington, D.C.; Goddard Space Flight Center in Greenbelt, Maryland; the Jet Propulsion Laboratory in Pasadena, California; the Marshall Space Flight Center in Huntsville, Alabama; and Ames Research Center at Moffett Field, California, from November 2008 to October 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: NASA Organization Chart



Source: NASA.

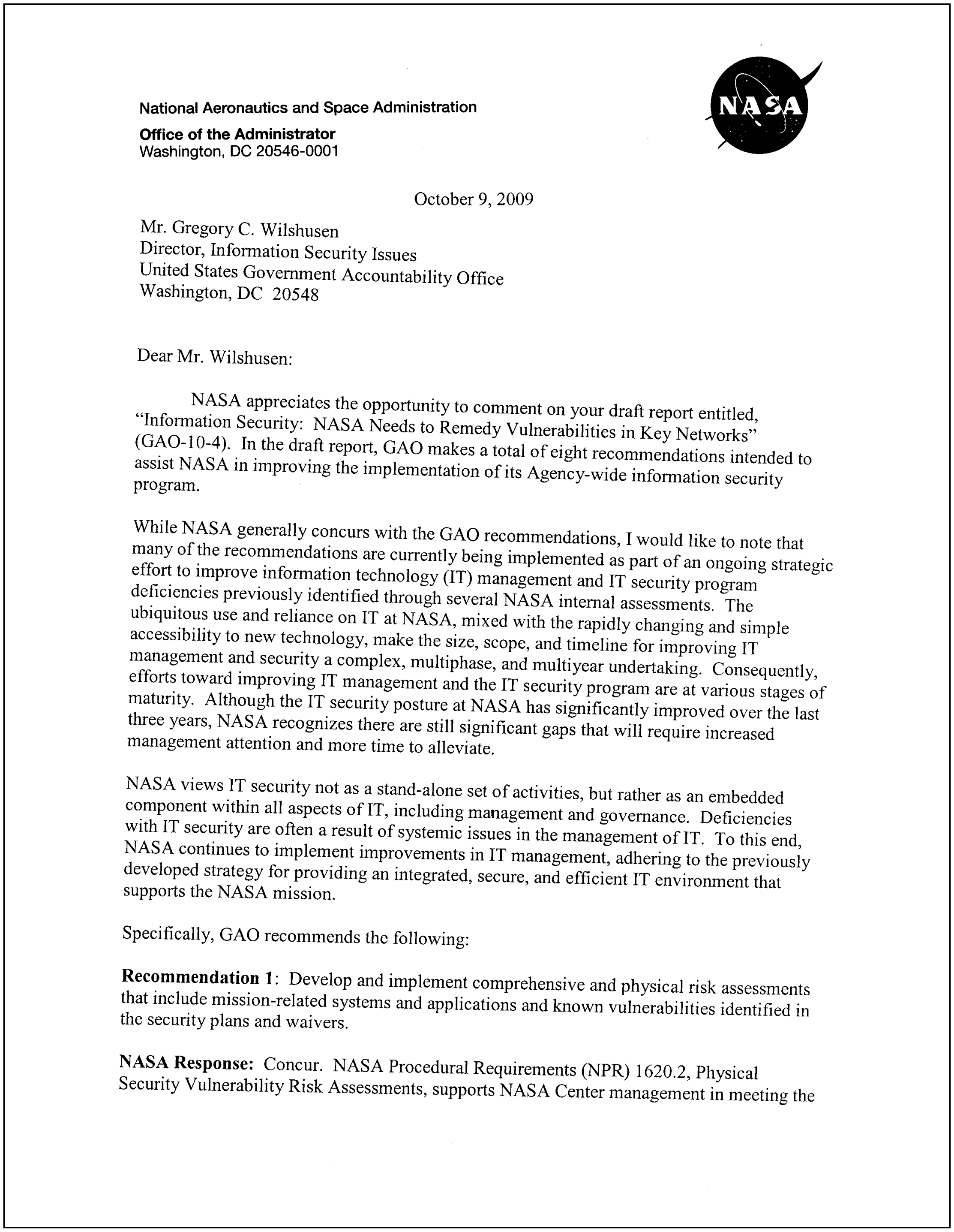
Appendix III: Missions of NASA Centers and the Jet Propulsion Laboratory

NASA center	Mission
Ames Research Center	Provides leadership in astrobiology, small-satellites, the search for habitable planets, supercomputing, intelligent/adaptive systems, advanced thermal protection, and airborne astronomy.
Dryden Flight Research Center	Performs flight research and technology integration to revolutionize aviation and pioneer aerospace technology; validates space exploration concepts; conducts airborne remote sensing, and science missions; enables airborne astrophysics observation missions to discover the origin, structure, evolution, and destiny of the universe; and supports operations of the Space Shuttle and the International Space Station.
Glenn Research Center	Develops critical space flight systems and technologies to advance the exploration of our solar system and beyond while maintaining leadership in aeronautics. In partnership with U.S. industries, universities, and other government institutions, research and development efforts focus on advancements in propulsion, power, communications, nuclear, and human-related aerospace systems.
Goddard Space Flight Center	Expands the knowledge of Earth and its environment, the solar system, and the universe through observations from space. The center also conducts scientific investigations, develops and operates space systems, and advances essential technologies.
Johnson Space Center	Hosts and staffs program and project offices; selects and trains astronauts; manages and conducts projects that build, test, and integrate human-rated systems for transportation, habitation, and working in space; and plans and operates human space flight missions. Programs that Johnson Space Center supports include the Space Shuttle Program, the International Space Station Program, and the Constellation Program.
Kennedy Space Center	Performs preflight processing, launch, landing, and recovery of the agency's human-rated spacecraft and launch vehicles; the assembly, integration, and processing of International Space Station elements and flight experiments; and the acquisition and management of Expendable Launch Vehicles for other agency spacecraft. The center leads the development of ground systems supporting human-rated spacecraft and launch vehicle hardware elements and hosts the manufacturing of the Orion Crew Exploration Vehicles.
Langley Research Center	Pioneers the future in space exploration, scientific discovery, and aeronautics through research and development of technology, scientific instruments and investigations, and exploration systems.
Marshall Space Flight Center	Performs systems engineering and integration for both human and robotic missions. Marshall performs engineering design, development, and integration of the systems required for space operations, exploration, and science. The center also manages the Michoud Assembly Facility, which supports the unique manufacturing and assembly needs of current and future NASA programs and provides critical telecommunications and business systems for the agency.
Stennis Space Center	Implements NASA's mission in areas assigned by three agency mission directorates. The center manages and operates Rocket Propulsion Test facilities and support infrastructure for the Space Operations and Exploration Systems mission directorates, serves as Systems Engineering Center for and manages assigned Applied Sciences program activities for the Science mission directorate, and serves as federal manager and host agency of a major government multiagency center.

NASA center	Mission
Jet Propulsion Laboratory	A contractor-operated federally funded research and development center that supports NASA's strategic goals by exploring our solar system; establishing a continuous permanent robotic presence at Mars to discover its history and habitability; making critical measurements and models to better understand the solid Earth, oceans, atmosphere, and ecosystems, and their interactions; conducting observations to search for neighboring solar systems and Earth-like planets, and help understand formation, evolution, and composition of the Universe; conducting communications and navigation for deep space missions; providing support that enables human exploration of the Moon, Mars, and beyond; and collaborating with other federal and state government agencies and commercial endeavors.

Source: GAO analysis of NASA data.

Appendix IV: Comments from NASA



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

October 9, 2009

Mr. Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

NASA appreciates the opportunity to comment on your draft report entitled, "Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks" (GAO-10-4). In the draft report, GAO makes a total of eight recommendations intended to assist NASA in improving the implementation of its Agency-wide information security program.

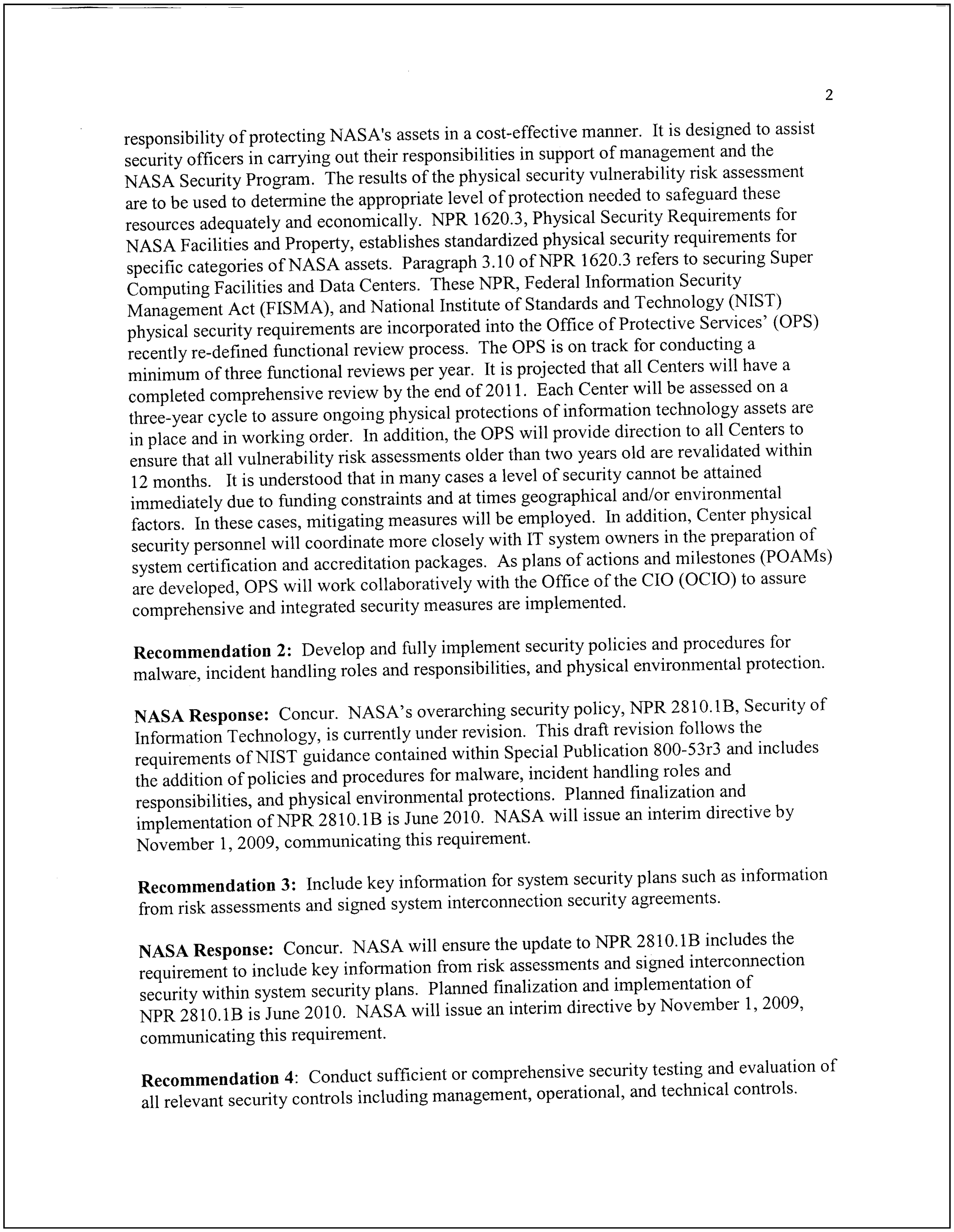
While NASA generally concurs with the GAO recommendations, I would like to note that many of the recommendations are currently being implemented as part of an ongoing strategic effort to improve information technology (IT) management and IT security program deficiencies previously identified through several NASA internal assessments. The ubiquitous use and reliance on IT at NASA, mixed with the rapidly changing and simple accessibility to new technology, make the size, scope, and timeline for improving IT management and security a complex, multiphase, and multiyear undertaking. Consequently, efforts toward improving IT management and the IT security program are at various stages of maturity. Although the IT security posture at NASA has significantly improved over the last three years, NASA recognizes there are still significant gaps that will require increased management attention and more time to alleviate.

NASA views IT security not as a stand-alone set of activities, but rather as an embedded component within all aspects of IT, including management and governance. Deficiencies with IT security are often a result of systemic issues in the management of IT. To this end, NASA continues to implement improvements in IT management, adhering to the previously developed strategy for providing an integrated, secure, and efficient IT environment that supports the NASA mission.

Specifically, GAO recommends the following:

Recommendation 1: Develop and implement comprehensive and physical risk assessments that include mission-related systems and applications and known vulnerabilities identified in the security plans and waivers.

NASA Response: Concur. NASA Procedural Requirements (NPR) 1620.2, Physical Security Vulnerability Risk Assessments, supports NASA Center management in meeting the



responsibility of protecting NASA's assets in a cost-effective manner. It is designed to assist security officers in carrying out their responsibilities in support of management and the NASA Security Program. The results of the physical security vulnerability risk assessment are to be used to determine the appropriate level of protection needed to safeguard these resources adequately and economically. NPR 1620.3, Physical Security Requirements for NASA Facilities and Property, establishes standardized physical security requirements for specific categories of NASA assets. Paragraph 3.10 of NPR 1620.3 refers to securing Super Computing Facilities and Data Centers. These NPR, Federal Information Security Management Act (FISMA), and National Institute of Standards and Technology (NIST) physical security requirements are incorporated into the Office of Protective Services' (OPS) recently re-defined functional review process. The OPS is on track for conducting a minimum of three functional reviews per year. It is projected that all Centers will have a completed comprehensive review by the end of 2011. Each Center will be assessed on a three-year cycle to assure ongoing physical protections of information technology assets are in place and in working order. In addition, the OPS will provide direction to all Centers to ensure that all vulnerability risk assessments older than two years old are revalidated within 12 months. It is understood that in many cases a level of security cannot be attained immediately due to funding constraints and at times geographical and/or environmental factors. In these cases, mitigating measures will be employed. In addition, Center physical security personnel will coordinate more closely with IT system owners in the preparation of system certification and accreditation packages. As plans of actions and milestones (POAMs) are developed, OPS will work collaboratively with the Office of the CIO (OCIO) to assure comprehensive and integrated security measures are implemented.

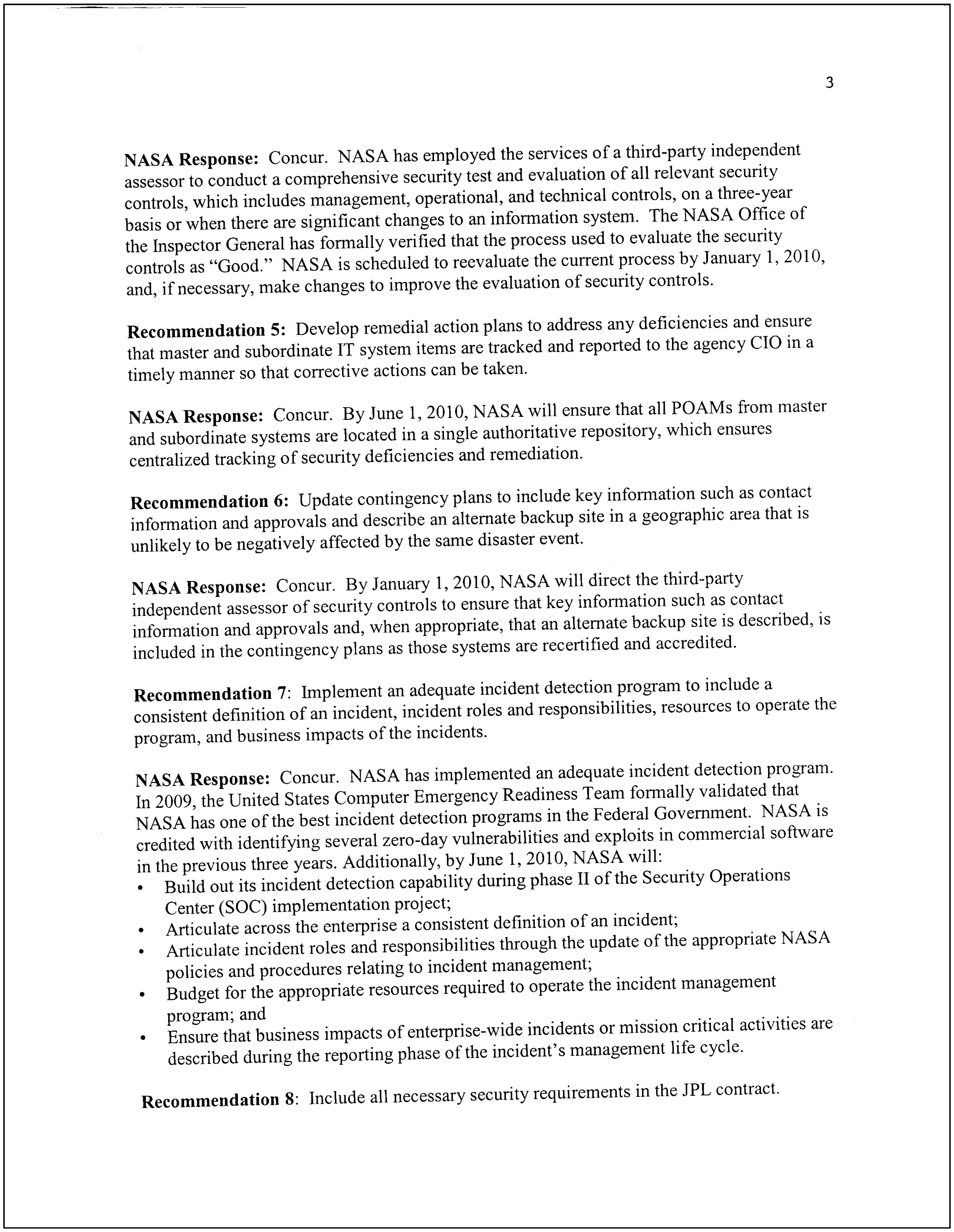
Recommendation 2: Develop and fully implement security policies and procedures for malware, incident handling roles and responsibilities, and physical environmental protection.

NASA Response: Concur. NASA's overarching security policy, NPR 2810.1B, Security of Information Technology, is currently under revision. This draft revision follows the requirements of NIST guidance contained within Special Publication 800-53r3 and includes the addition of policies and procedures for malware, incident handling roles and responsibilities, and physical environmental protections. Planned finalization and implementation of NPR 2810.1B is June 2010. NASA will issue an interim directive by November 1, 2009, communicating this requirement.

Recommendation 3: Include key information for system security plans such as information from risk assessments and signed system interconnection security agreements.

NASA Response: Concur. NASA will ensure the update to NPR 2810.1B includes the requirement to include key information from risk assessments and signed interconnection security within system security plans. Planned finalization and implementation of NPR 2810.1B is June 2010. NASA will issue an interim directive by November 1, 2009, communicating this requirement.

Recommendation 4: Conduct sufficient or comprehensive security testing and evaluation of all relevant security controls including management, operational, and technical controls.



NASA Response: Concur. NASA has employed the services of a third-party independent assessor to conduct a comprehensive security test and evaluation of all relevant security controls, which includes management, operational, and technical controls, on a three-year basis or when there are significant changes to an information system. The NASA Office of the Inspector General has formally verified that the process used to evaluate the security controls as "Good." NASA is scheduled to reevaluate the current process by January 1, 2010, and, if necessary, make changes to improve the evaluation of security controls.

Recommendation 5: Develop remedial action plans to address any deficiencies and ensure that master and subordinate IT system items are tracked and reported to the agency CIO in a timely manner so that corrective actions can be taken.

NASA Response: Concur. By June 1, 2010, NASA will ensure that all POAMs from master and subordinate systems are located in a single authoritative repository, which ensures centralized tracking of security deficiencies and remediation.

Recommendation 6: Update contingency plans to include key information such as contact information and approvals and describe an alternate backup site in a geographic area that is unlikely to be negatively affected by the same disaster event.

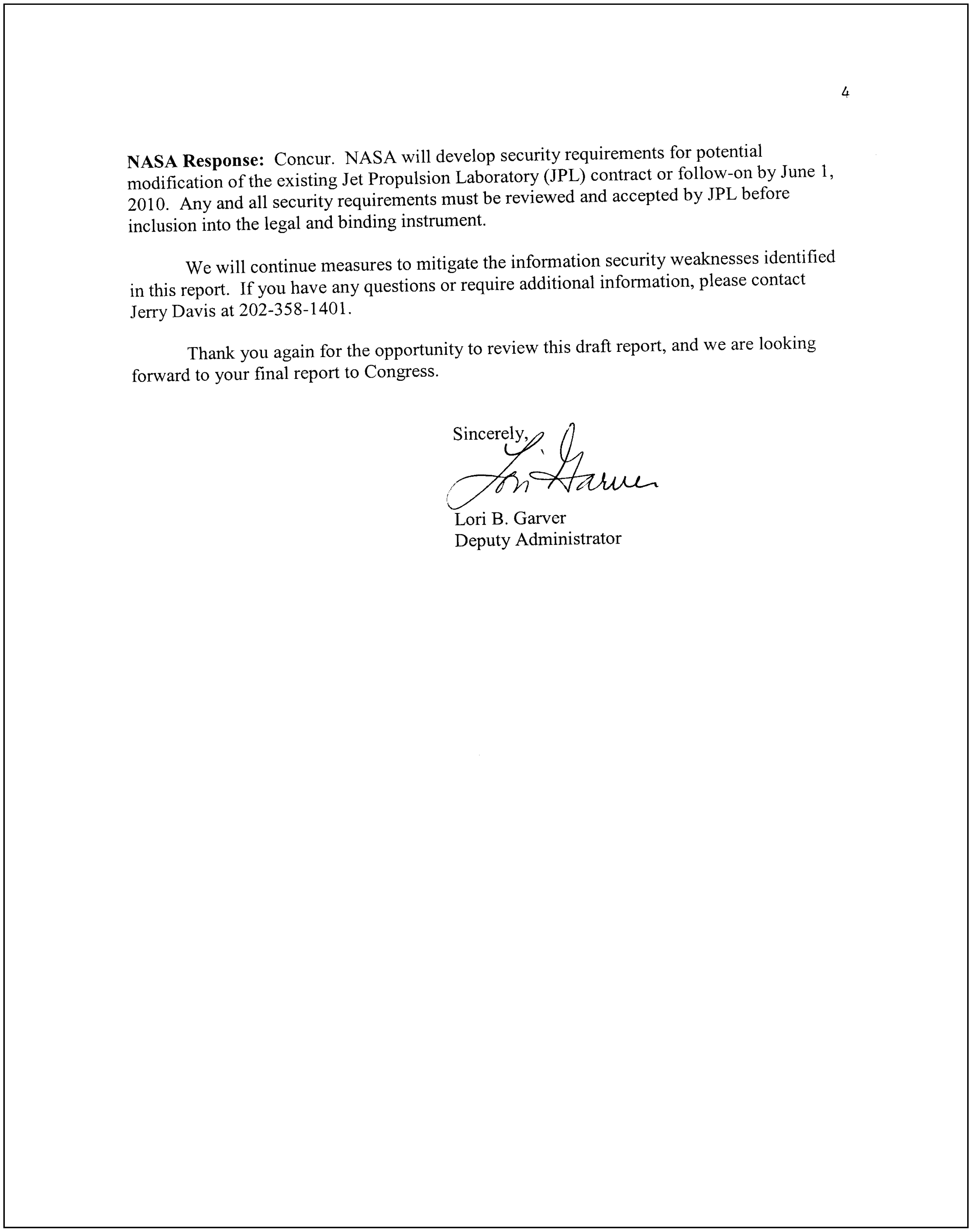
NASA Response: Concur. By January 1, 2010, NASA will direct the third-party independent assessor of security controls to ensure that key information such as contact information and approvals and, when appropriate, that an alternate backup site is described, is included in the contingency plans as those systems are recertified and accredited.

Recommendation 7: Implement an adequate incident detection program to include a consistent definition of an incident, incident roles and responsibilities, resources to operate the program, and business impacts of the incidents.

NASA Response: Concur. NASA has implemented an adequate incident detection program. In 2009, the United States Computer Emergency Readiness Team formally validated that NASA has one of the best incident detection programs in the Federal Government. NASA is credited with identifying several zero-day vulnerabilities and exploits in commercial software in the previous three years. Additionally, by June 1, 2010, NASA will:

- Build out its incident detection capability during phase II of the Security Operations Center (SOC) implementation project;
- Articulate across the enterprise a consistent definition of an incident;
- Articulate incident roles and responsibilities through the update of the appropriate NASA policies and procedures relating to incident management;
- Budget for the appropriate resources required to operate the incident management program; and
- Ensure that business impacts of enterprise-wide incidents or mission critical activities are described during the reporting phase of the incident's management life cycle.

Recommendation 8: Include all necessary security requirements in the JPL contract.



NASA Response: Concur. NASA will develop security requirements for potential modification of the existing Jet Propulsion Laboratory (JPL) contract or follow-on by June 1, 2010. Any and all security requirements must be reviewed and accepted by JPL before inclusion into the legal and binding instrument.

We will continue measures to mitigate the information security weaknesses identified in this report. If you have any questions or require additional information, please contact Jerry Davis at 202-358-1401.

Thank you again for the opportunity to review this draft report, and we are looking forward to your final report to Congress.

Sincerely,

Lori B. Garver
Deputy Administrator

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, or wilshuseng@gao.gov
Dr. Nabajyoti Barkakati, (202) 512-4499, or barkakatin@gao.gov

Staff Acknowledgments

In addition to the individuals named above, West Coile and William Wadsworth (Assistant Directors), Edward Alexander, Angela Bell, Mark Canter, Saar Dagani, Kirk Daubenspeck, Neil Doherty, Patrick Dugan, Denise Fitzpatrick, Edward Glagola Jr., Tammi Kalugdan, Vernetta Marquis, Sean Mays, Lee McCracken, Kevin Metcalfe, Duc Ngo, Donald Sebers, Eugene Stevens IV, Michael Stevens, Henry Sutanto, Christopher Warweg, and Jayne Wilson made key contributions to this report.

(311032)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548