October 2009

INFORMATION SECURITY

NASA Needs to Remedy Vulnerabilities in Key Networks

GAO 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.

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.