

Audit Report, "Security of [a NASA Center's Computer] Network" (IG-06-008, June 2, 2006)

The NASA Office of Inspector General conducted an audit to determine whether [a NASA Center] had implemented adequate information technology security controls to provide reasonable assurance of network security to protect NASA data and systems against possible compromise.

The NASA Center's controls did not provide reasonable assurance of network security. Specifically, system administrators did not (1) periodically review critical firewall audit logs and modems used to protect the computer network; (2) monitor for the use of files and commands with security risks; (3) consistently perform system backups; and (4) meet NASA requirements for storing backup media. System administrators also accessed a key server containing security information without adequate encryption and did not remove unnecessary services from the network. Further, software patches were not timely installed to fix security weaknesses in the network servers and vulnerabilities found during security scans of the systems were not corrected in a timely manner. Finally, NASA did not have a formal policy for laptops or other electronic devices used by foreign nationals visiting the NASA Center or working onsite. Weaknesses in these areas could lead to the compromise of the computer network.

We recommended that the NASA Center take actions to improve security controls over the network, to include developing, implementing, and enforcing procedures and controls over auditing and monitoring, the use of software and unnecessary services, the installation of patches, and system backups. We also recommended that the Center develop and implement a formal policy to prohibit foreign nationals' onsite use of their own laptops and other electronic devices.

NASA concurred with 9 of our 13 recommendations and had taken or planned corrective actions to improve security controls over the computer network. We considered management's actions to be responsive to eight of those nine recommendations. Of the eight, we closed four recommendations and considered four resolved but open pending verification of the proposed actions. In addition, of the four recommendations with which management nonconcurred, we considered the proposed corrective actions for three to be responsive and have closed those recommendations.

We did not consider management's comments on two recommendations to be responsive and requested additional comments in response to the final report.

*The report contains NASA Information Technology/Internal Systems Data that is not routinely released under the Freedom of Information Act (FOIA). To submit a FOIA request, see the [online guide](#).*