Audit Report, "Review of the Information Technology Security of [a NASA Computer Network]" (IG-10-013, May 13, 2010); addendum issued July 1, 2010

We evaluated the processes for continuously monitoring selected information technology (IT) security controls on a NASA mission computer network. Specifically, we assessed whether processes were in place to implement software patches and to identify and remediate technical vulnerabilities. We found that NASA did not adequately protect the network from potential security breaches and did not always ensure that key IT security controls were monitored.

We recommended that the NASA Chief Information Officer designate a NASA Directorate or Center to immediately establish an oversight process for the network to include monitoring of systems connected to the network for the presence of critical patches and technical vulnerabilities and review all other Agency mission network IT security programs to determine whether each contains an effective oversight process.

The Office of the Chief Information Officer (OCIO) partially concurred with both report recommendations; however, management's planned actions were not fully responsive to the intent of our recommendations. Additional comments received in June 2010 stated that NASA plans to complete the following actions:

- issue a memorandum to Mission Directorates, Centers, and system owners describing processes and procedures for vulnerability scanning and remediation;
- establish an integrated Agency oversight process to coordinate existing activities and formalize channels of communication; and
- implement a centralized data repository to support Agency oversight of mission computer networks.

The additional comments are responsive, and the recommendations are resolved.

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.