

Federal Information Security Management Act: Fiscal Year 2012 Evaluation
(IG-13-001, October 10, 2012)

This annual report, submitted as a memorandum from the Inspector General to the NASA Administrator, provides the Office of Inspector General's (OIG) independent assessment of NASA's information technology (IT) security posture. For FY 2012, the OIG adopted a risk-based approach under which we reviewed a sample of 129 system components monitored by automated tools across NASA and performed a manual review of five mission systems (two Agency internal and three external information systems).

Overall, we found that NASA has established a program to address the challenges in each of the areas that the Office of Management and Budget (OMB) identified for this year's Federal Information Security Management Act (FISMA) review. However, the Agency needs to make more progress in addressing NASA's continuous monitoring management, configuration management, and risk management issues.

Our report addressed the 11 required areas of review for FY 2012 FISMA reporting:

- Continuous Monitoring Management
- Configuration Management
- Identity and Access Management
- Incident Response and Reporting
- Risk Management
- Security Training
- Plan of Action and Milestones (POA&M)
- Remote Access Management
- Contingency Planning
- Contractor Systems
- Security Capital Planning

The OIG concluded that IT security will remain a significant challenge for the Agency as it moves from a compliance-focused, "snapshot" approach for measuring the security of its IT systems to using tools and techniques to perform real-time monitoring. During FY 2013 and beyond, the OIG will continue to assess NASA's IT security program through focused audits of discrete IT security issues, such as the security of mobile devices and cloud-computing technologies, as well as through our annual FISMA reviews.

The OMB will provide a consolidated report to Congress, which will include information from our report. However, as an "Intra-Agency Memorandum" our report is considered exempt from release under the Freedom of Information Act (FOIA); it also contains NASA Information Technology/Internal Systems Data that is considered Sensitive But Unclassified and therefore not routinely released under FOIA. To submit a FOIA request, see the [online guide](#).

OMB's report is made available over the Internet (last year's, [Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002](#), was released by OMB in March 2012).