Federal Information Security Modernization Act: Fiscal Year 2016 Evaluation (IG-17-002, November 7, 2016)

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 security posture, as required by the Federal Information Security Modernization Act of 2014 (FISMA). The law identifies specific security requirements Federal agencies must satisfy and assigns responsibilities to agency officials for addressing and Inspectors General for assessing these requirements. For example, agency officials are responsible for developing policies and procedures commensurate with the risk and magnitude of harm from malicious or unintentional impairment of agency information and information systems, while Inspectors General are responsible for performing independent evaluations examining the effectiveness of their agencies' information security program and practices.

FISMA requires the OIG test a representative subset of NASA's systems. For fiscal year (FY) 2016, we used a risk-based approach to examine a sample of five Agency and contractor information systems. We also considered findings from previous OIG audit work in reaching our conclusions.

The 2016 OIG FISMA reporting requirements are organized around five functions critical to an effective information security program:

1. *Identify.* Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2. *Protect*. Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
3. *Detect*. Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4. *Respond*. Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5. *Recover.* Develop and implement the appropriate activities to maintain plans for resilience and to restore capabilities or services impaired due to a cybersecurity event.

Together, these functions provide a strategic view of the lifecycle of an organization's cybersecurity risk management.

The Office of Management and Budget (OMB) and the Department of Homeland Security developed a scoring system with point allocations for each of the functions. Agencies are allotted up to 20 points for each function up to a total of 100 points, which would represent a fully effective information security system. Agencies accumulate points by satisfying metrics associated with attainment of the five functions and, accordingly, the more mature an agency's efforts on a particular function, the higher its score for that function.

Overall, we determined that NASA lacks an effective program in any of the five functions, earning 27 of the possible 100 maturity level points. NASA earned 3 points each for the Protect and Detect functions, indicating it lacks formalized programs in those areas and performs activities in a reactive rather than proactive manner. For the other the three functions NASA scored 7 points each, indicating it has formalized programs in those areas but fails to consistently implement them Agency-wide. That said, we noted NASA has several efforts underway in each of the functional areas to improve its information security program.

By implementing previous OIG audit recommendations and taking additional actions, NASA is working to improve its overall information security posture. Nevertheless, as indicated by the results of this review, information security remains a top management challenge for the Agency. Moving forward, we will continue to examine NASA's information security program both through focused audits of discrete issues and future FISMA reviews.

OMB is expected to issue its Government-wide consolidated FISMA report, which will include information from our report, in the Spring of 2017.