NASA Advisory Council Recommendation

Information Technology (IT) Security Risk Management Structure
2016-01-02 (IC-01)

Recommendation:
The Council recommends that NASA accelerate the schedule to develop an IT Security Risk Management structure from its current schedule completion date of December 31, 2017, to an earlier date.

Major Reasons for Proposing the Recommendation:
The Agency would benefit from formalizing an IT Security Risk Management Framework and Cybersecurity Strategy to more effectively deploy limited resources. This is required to enable informed decisions on investments and planned actions.

Consequences of No Action on the Proposed Recommendation:
If this recommendation is not accepted there could be a non-optimal deployment of resources applied to NASA cybersecurity efforts.

NASA Response:
NASA concurs with this recommendation. The Office of Chief Information Officer has developed a comprehensive approach to implementing an integrated IT security risk management strategy for IT systems that defines roles, responsibilities, and assessment methodology across the Agency from the IT system owner to the Agency Chief Information Officer, as well as implementing a holistic IT Security Risk Management System that will provide near real-time monitoring and vulnerability and risk profile.

On March 31, 2016, NASA's Mission Support Council approved, through the Business Services Assessment Initiative, the IT Security Risk Management Strategy and Architecture solution. The implementation of NASA's IT Risk Management strategy began in the third quarter of FY 2016 with the design and implementation of a Commercial-Off-The-Shelf (COTS) product (RSA Archer) to improve the management IT technical risk across all of NASA's IT systems. The anticipated institutionalization of NASA's Risk Information and Security System (RISCS) will allow for a more robust assessment and remediation processes by starting operations September 30, 2016. Full operational capability to track, assess, and report IT technical security risk is now planned for December 31, 2016. The RISCS system will provide vital vulnerability, system security plan, and Continuous Diagnostics and Mitigation (CDM) sensor information, which will enable management to make better decisions on mitigations of IT risk, and provide a consistent process for evaluating and improving the overall risk profile of the Agency.

Enclosure