Federal Information Security Management Act: FY 2015 Evaluation

The Federal Information Security Modernization Act of 2014 (FISMA)[1] requires the Office of Inspector General (OIG) to conduct an independent evaluation to assess the effectiveness of NSF's information security program and practices and to determine compliance with FISMA requirements. The OIG contracted for the FY 2015 FISMA evaluation.

Areas reviewed in FY 2015 included NSF's financial accounting and grants management systems, including iTRAK (NSF's core financial system), the NSF website, and the systems supporting NSF's United States Antarctic Program (USAP).

The FY 2015 evaluation included twenty-two findings; fourteen new findings and eight repeat findings from prior years. Two of the repeat findings, both of which remain open, are from FY 2010 or earlier. The first finding, first reported in FY 2006, pertained to USAP, which is managed by NSF's Division of Polar Programs and its contractor Lockheed Martin. Valued at nearly $2 billion over 13 years, the Antarctic Support Contract is NSF's largest contract. The finding related to disaster recovery plans for the USAP systems. The second finding, first reported in FY 2010, pertained to NSF's controls for ensuring that IT access for separated employees and contractors was terminated in a timely manner.

Other repeat findings, which remain open, included weaknesses in NSF's IT configuration management controls, which increase risk that unauthorized changes could occur and go undetected; interagency support agreements related to the USAP interconnections, which could lead to undetected failures in the connections; and weaknesses in incident response controls, which could lead to unauthorized access to sensitive information.

The fourteen new findings cited in the FY 2015 report included twelve findings for NSF and two for USAP. Of the twelve new NSF findings, eight related to iTRAK, NSF's recently-implemented core financial system. Three of the new findings (one each for the NSF, iTRAK, and USAP systems) related to account management and background investigations, which could lead to unauthorized access to systems and data across the agency, and expose NSF to the risk of inadvertent or deliberate compromise to the confidentiality, integrity, and availability of its systems and data.

The other new findings for iTRAK included weaknesses in configuration and patch management, which could increase the risk of unauthorized changes to the system; weaknesses in audit and accountability controls, which could increase the risk that unusual or unauthorized activity could occur undetected; and weaknesses in recovery procedures and processes, which could increase the risk that systems may not be adequately restored in a timely manner during disasters.

The new findings for NSF included weaknesses in system security plans, which could increase the risk that unauthorized changes could occur undetected; and the Plan of Actions and

[1] The Federal Information Security Modernization Act of 2014 amends the FISMA Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security to administer the implementation of such policies and practices for information systems.

Milestones Process (POA&M), which could increase the risk that vulnerabilities are not appropriately remediated. The new findings for the USAP systems included weaknesses in assessment and authorization documentation, which could increase the risk that appropriate security controls will not be consistently applied.

NSF depends on computerized information systems to execute its scientific research and operations and to process, maintain, and report essential information. Reliability of computerized data and systems is essential and protecting information systems continues to be a challenge for NSF. The FY 2015 FISMA report recommends a number of actions necessary for NSF to continue to strengthen IT security.

The auditors also issued a Management Letter to NSF, which reviewed the status of NSF's corrective actions to address FY 2014 findings. The auditors concluded that NSF had improved IT security and recommended management's continued attention to further strengthening controls and to implementing recommendations from prior FISMA reports.