Federal Information Security Management Act: FY 2014 Evaluation

The Federal Information Security Management Act (FISMA) 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.

Areas reviewed in FY 2014 included NSF's financial accounting and grants management systems and the NSF website as well as systems supporting NSF's United States Antarctic Program (USAP).

The FY 2014 evaluation included a total of nineteen findings; eight new findings and eleven repeat findings from prior years. Three of the repeat findings, all of which remain open, are from FY 2010 or earlier. Two of these findings, both from FY 2006, pertained to USAP, which is managed by the 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 findings related to USAP's operating environment and disaster recovery plans. The third such finding, from 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, and weaknesses in incident response controls, which could lead to unauthorized access to sensitive information.

The eight new findings cited in the FY 2014 report included six findings for NSF and two for USAP. Findings for NSF included weaknesses in contingency planning, which could increase the risk that systems may not be adequately restored in a timely manner during disasters, and delays in correcting critical system vulnerabilities, which increase the risk of IT systems being compromised. The new findings for the USAP related to weaknesses in controls to disable inactive accounts, which increase the risk that individuals may obtain unauthorized access to USAP systems, and inconsistent screening of personal computers.

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 2014 FISMA report recommends a number of actions necessary for NSF to continue to strengthen IT security.