Office of Inspector General
U.S. Government Accountability Office
Report Highlights
Accessible Version

July 17, 2018

INFORMATION SECURITY

Review of GAO's Program and Practices for Fiscal Years 2016 and 2017

Objective

Our audit objective was to assess GAO's compliance with Federal Information Security Modernization Act of 2014 (FISMA) requirements.

What OIG Found

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program for the information and systems that support their operations and assets, including those provided or managed by another agency or contractor. GAO is not obligated by law to comply with FISMA or executive branch information security policies, but has adopted them to help ensure its physical and information system security. Our work has continued to confirm ongoing progress in GAO's efforts to refine its information security program in a manner that is generally consistent with the requirements of FISMA, Office of Management and Budget implementing guidance, and National Institute of Standards and Technology standards and guidance. GAO also has a robust information security awareness training program. During the period reviewed, GAO continued efforts to improve upon existing capabilities and strengthen its information security controls, particularly in the areas of identity and access management, security training, and continuous monitoring. Our report identifies specific areas, such as configuration management and contingency planning, where additional efforts are needed to further strengthen GAO's information security consistent with FISMA requirements. The issues we identified in this report also highlight how gaps in GAO's implementation of an enterprise-wide risk management program may have contributed to the challenges and heightened risks identified during our audit.

Due to the sensitive nature of our findings, a full report on the results of our audit was prepared for internal GAO use only during our audit.

What OIG Recommends

The OIG is making three recommendations to the Comptroller General intended to help the GAO more fully implement federal information security requirements. Specifically, we recommend that GAO document (1) a process to evaluate current and future enterprise IT investment portfolio assets, including risks, and ensure alignment with GAO's IT Strategy for fiscal years 2017-2019 and (2) its plans, policies, and procedures for identifying, prioritizing, and mitigating operational risk related to establishing full failover capabilities at the agency's alternate computing facility in the event of a disaster and preparing for end-of-support upgrades for Windows 7. In addition, we recommend that GAO document and implement a process to identify and track hardware and software interdependencies for GAO's system inventory including vendor support data. GAO agreed with our recommendations and described actions planned to mitigate the control risks identified in our work. The agency also provided technical comments that we incorporated, as appropriate.