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

March 28, 2016

INFORMATION SECURITY

Review of GAO's Program and Practices for Fiscal Years 2014 and 2015

Objective

Our audit objective was to assess GAO's compliance with Federal Information Security Management Act of 2002 (FISMA) requirements.

What OIG Found

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program to provide security 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. Our work found that GAO has established an overall information security program that is generally consistent with the requirements of FISMA, OMB guidance, and standards and guidance issued by the National Institute of Standards and Technology. In addition, GAO has taken important steps to improve its security posture in response to recent federal cyber incidents. Our report identifies key areas, such as configuration management, contingency planning, and risk management, where additional steps could be taken in to more fully comply with federal information security requirements and to strengthen GAO's information security framework consistent with best practices.

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

What OIG Recommends

We made six recommendations to the Comptroller General to further strengthen GAO's information security program. We recommend that GAO take action to mitigate identified configuration management weaknesses, enhance its contingency planning to ensure its alternative computing facility has the ability to quickly take over system operations for all mission-essential information systems and components in the event of a disruption, and strengthen its framework for identifying and managing risk at an enterprise level. GAO agreed with our recommendations and described actions planned to mitigate the control risks identified in our work.