Accessible Version

Office of Inspector General
U.S. Government Accountability Office
September 30, 2019

INFORMATION SECURITY
Review of GAO's Program and Practices for Fiscal Year 2018

Report Highlights

Objective

This report presents the OIG's assessment of 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. Although GAO, as a legislative branch agency, is not subject to FISMA, its management has chosen to use FISMA as a set of best practices for its information security program. GAO has defined an information security program that is generally aligned with FISMA, however the OIG identified several opportunities for GAO to improve the implementation of its information security program and to ensure alignment with federal best practices.

While GAO continues to make progress in developing its organizational capability for understanding and managing cybersecurity risk, it faces challenges in three areas. The design of GAO's enterprise risk management program is largely consistent with National Institute of Standards and Technology (NIST) guidance although GAO has not fully implemented controls in the areas of Risk Management Strategy, Risk Assessment, and Supply Chain Risk Management. Specifically,

- GAO has established an enterprise risk management (ERM) program that defines the organization's risk management strategy; however, GAO needs to better define its risk appetite, including risk tolerances.

- Risk has not been assessed on all GAO systems. Although GAO has established a program to assess system risk, it has not been fully implemented. The assessment process includes categorizing the impact level of the system and creating a system security plan, if required.

- GAO policy requires that specific Information Technology (IT) security and privacy requirements be included in all contracts and based on the particular nature of the IT services and the data requirements of the contract. However, the procedures that GAO developed for security and privacy requirements did not address NIST recommendations for ensuring contracts meet security requirements.

Additionally, GAO has generally established information protection policies that are consistent with federal best practices but has not consistently implemented these policies and procedures. For example, GAO regularly scans its environments to discover vulnerabilities such as

misconfigurations and missing patches. However, critical and high priority vulnerabilities were not always remediated in a timely fashion. Also, GAO policies call for establishing baseline configurations that can be used to configure machines securely and detect changes in the environment, but many were not documented.

The OIG also identified opportunities for GAO to improve disaster recovery planning. GAO did not conduct a disaster recovery plan test in fiscal year 2018, and one high-impact system did not have a contingency plan defined. Finally, GAO did not complete a business impact analysis which helps to inform contingency planning decisions.

This report is being released in summary form due to the sensitive nature of the subject matter.

What OIG Recommends

The OIG is making eight recommendations to strengthen GAO's information security program and practices. We recommend that GAO (1) finalize a key input to GAO's Enterprise Risk Management Strategy, specifically the risk appetite statement including risk tolerances; (2) review all entries in GAO's system inventory to determine if an impact assessment is needed and that assessments are performed as appropriate; (3) update standard operating procedures to ensure that standard contract language for security aligns with NIST recommendations as appropriate; (4) remediate identified vulnerabilities within prescribed time frames; (5) document and approve baseline configurations for all identified environments; (6) ensure that contingency planning testing accurately reflects the ability of GAO to recover mission critical systems in the event of a disaster; (7) document and approve a contingency plan for all high-impact systems; and (8) complete a business impact analysis for IT systems and update contingency plans where necessary to ensure that business needs are met in the event of a disaster. Management fully agreed with six of the eight findings and has identified actions taken or planned actions for the associated recommendations. For one of the findings (Rec. 4), GAO agreed with the finding but has not yet identified an action to be taken in response. For the remaining finding (Rec. 8), GAO disagreed with the finding but has stated that they will be taking action to address the associated recommendation.