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

March 31, 2022

INFORMATION SECURITY

Privacy Program Improvements Could Enhance GAO Efforts to Protect Data and Systems

Objective

This report presents the OIG's Fiscal Year (FY) 2021 assessment of the effectiveness of GAO's information security program in relation to selected Federal Information Security Modernization Act of 2014 (FISMA) requirements.

What OIG Found

We assessed GAO's information systems against selected FY 2021 Inspector General (IG) FISMA reporting metrics, and found certain aspects pertaining to management of data protection and privacy have opportunities for improvement. While GAO has taken steps to protect sensitive information and prevent data exfiltration, opportunities exist to improve its privacy program in the areas of incident response and training for people with specific roles.

- GAO's Incident Response plan does not contain all the recommended elements for addressing incidents involving Personally Identifiable Information (PII). Specifically, the current GAO incident response procedures do not contain documented procedures for assessing the potential damage to organizations and individuals resulting from the loss of PII.
- All GAO employees and contractors receive privacy training annually, as part of a mandatory course on security and privacy awareness. However, we found that training for personnel with role-specific responsibility for PII has not been consistently implemented.

During a penetration test we performed to assess the effectiveness of controls in the configuration management and information security continuous monitoring categories, we did not identify any significant vulnerabilities that would result in substantial compromise. We also found that GAO's policies and procedures for security training and its approach to identity and access management generally align with NIST guidance.

What OIG Recommends

We recommend that the Comptroller General direct the Chief Administrative Officer to direct the appropriate office(s) to (1) define and implement policies and procedures for incident response that align with NIST guidance for assessing privacy impact incidents and (2) define and implement policies and procedures for role-based privacy training which (a) identify who must regularly take the training, and (b) ensure annual compliance with such training. GAO agreed with the recommendations and outlined planned actions to address them.