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

February 2013

INFORMATION SECURITY

Evaluation of GAO's Program and Practices for Fiscal Year 2012

What We Found

The Federal Information Security Management Act of 2002 (FISMA) requires that each federal agency establish an agency-wide information security management program for the information and information systems that support the agency's operations and assets. GAO is not obligated by law to comply with FISMA or Executive Branch information policies, but has adopted them to help ensure physical and information system security. Our prior year evaluations have shown that GAO has established an overall information security program that is generally consistent with the requirements of FISMA, OMB implementing guidance, and standards and guidance issued by the National Institute of Standards and Technology. For example, GAO has well defined operational and technical controls for remote access to its network. Its telecommunications policy requires users to sign rules of behavior and user agreements that acknowledge their responsibility and accountability. GAO also has a process for reporting and disabling lost or stolen devices to prevent unauthorized access. In addition, GAO has continued its focus on closing prior year security-related recommendations.

Our fiscal year 2012 limited evaluation reinforced our prior conclusion. However, using 18 new FISMA reporting metrics for federal inspectors general, we identified areas for improvement in the contingency planning process. We also identified resource challenges that affect GAO's ability to implement security upgrades and strategies identified by GAO managers and the OIG.

What We Recommend

To help strengthen GAO's overall information security program, we recommend that the Chief Information Officer take the following two actions: (1) implement measures to increase the redundancy and availability of GAO mission-essential applications and (2) develop and provide, for GAO senior management consideration, a proposed strategy to ensure power redundancy to GAO servers and provide a long-term alternate power supply in the event of a power outage. GAO concurred with our recommendations.