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

March 2012

INFORMATION SECURITY

Evaluation for GAO's Program and Practices for Fiscal Year 2011

What We Found

The Federal Information Security Management Act of 2002 (FISMA) requires that each federal agency establish an agencywide 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 evaluation showed that GAO has established an overall information security program that is generally consistent with the requirements of FISMA, Office of Management and Budget implementing guidance, and standards and guidance issued by the National Institute of Standards and Technology. However, using FISMA reporting metrics for federal inspectors general, we identified opportunities to improve specific elements of this program that concern

- addressing information security risk from an overall agency perspective through a comprehensive governance structure and organization-wide risk management strategy,
- remediating security weaknesses identified for agency information systems in a timely manner,
- building out GAO's Alternative Computing Facility to fully support the agency's mission-essential functions in the event of an emergency or disaster, and
- developing accurate statistics for employees and contractors completing annual security awareness and role-based training.

A full report on this evaluation was prepared for internal GAO use only.

What We Recommend

This report recommends that GAO (1) establish a comprehensive governance structure and organization-wide risk management strategy for the security of its information systems; (2) enhance accountability for, and management of, the agency's information security weakness remediation process; (3) provide senior management with adequate information to consider and prioritize building out the capabilities of the agency's Alternative Computing Facility; and (4) develop and implement procedures for capturing data that accurately reflect agency compliance with security training requirements as of the end of each fiscal year. GAO concurred with these recommendations.

Reporting Fraud, Waste, and Abuse in GAO's Internal Operations

To report fraud, waste, and abuse in GAO's internal operations, do one of the following. (You may do so anonymously.)

- Call toll-free (866) 680-7963 to speak with a hotline specialist, available 24 hours a day, 7 days a week.
- Online at: https://OIG.alertline.com.

Obtaining Copies of OIG Reports and Testimony

To obtain copies of OIG reports and testimony, go to GAO's Web site: www.gao.gov/about/workforce/ig.html.

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548