GAO

Accountability ★ Integrity ★ Reliability

OIG

Highlights

March 2011

INFORMATION SECURITY

Evaluation of GAO's Program and Practices for Fiscal Year 2010

Objectives: GAO is not obligated by law to comply with, but has adopted, the requirements of the Federal Information Security Management Act of 2002 (FISMA) to strengthen its information security program and demonstrate its ongoing commitment to lead by example. GAO's Office of Inspector General (OIG) conducted an evaluation to assess (1) the effectiveness of the agency's information security policies, procedures, and practices, and (2) agency compliance with the information security requirements of FISMA and other federal information security policies, procedures, standards, and guidelines. (A full report on this evaluation was prepared for GAO internal use only.)

Findings: The OIG's evaluation showed that GAO has established an information security program that is generally consistent with the requirements of FISMA, Office of Management and Budget (OMB) implementing guidance, and standards and guidance issued by the National Institute of Standards and Technology. However, using evaluation metrics provided by OMB for inspectors general, the OIG also identified improvement opportunities for specific elements of this program that concern

- identifying the agency's systems inventory and assuring that all systems operated by GAO or by contractors meet security requirements,
- implementing additional computer scanning capabilities to test security configuration settings,
- remediating configuration-related vulnerabilities in a timely manner,
- ensuring that contractors have access to required role-based security awareness training, and
- planning for further implementation of the personal identity verification requirements of Homeland Security Presidential Directive 12 (HSPD-12).

Recommendations: This report recommends that GAO (1) incorporate procedures within its annual systems inventory process that require inventory changes to be documented and formally approved by the Chief Information Officer and that system interfaces be identified, (2) identify and pursue additional options for obtaining assurances that certain contractor systems meet federal information security requirements, (3) continue efforts to complete and document required information security processes and procedures for all GAO-operated systems, (4) proceed with plans to establish a security configuration scanning capability for GAO notebook computers and workstations, (5) incorporate changes to the configuration management process that remediate specific open configuration-related vulnerabilities, (6) ensure that access to annual role-based information security training or its equivalent is provided for all contractor staff required to take this training, and (7) develop and brief senior management on a plan for practical implementation of HSPD-12 requirements. 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.
- Send an e-mail to OIGHotline@gao.gov.
- Send a fax to the OIG Fraud, Waste, and Abuse Hotline at (202) 512-8361.
- Write to:

GAO Office of Inspector General
441 G Street NW, Room 1808
Washington, DC 20548

Obtaining Copies of GAO/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

Ralph Dawn, Managing Director, dawnr@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