GAO
Accountability ★ Integrity ★ Reliability
OIG
Highlights

January 4, 2010

INFORMATION SECURITY

Evaluation of GAO’s Information Security Program and Practices for Fiscal Year 2009

Objectives: Although not obligated by law to comply, GAO 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 our evaluation was prepared for GAO internal use only.)

Findings: Overall, the OIG’s evaluation showed that GAO has established an information security program consistent with the requirements of FISMA, Office of Management and Budget (OMB) implementing guidance, and guidance and standards issued by the National Institute of Standards and Technology (NIST). However, it also found that GAO’s information security policies and procedures were not always applied and some could be improved to help ensure that they are consistent with the OMB and NIST guidance. In particular, the OIG found the following:

- During fiscal year 2009, GAO greatly increased its systems inventory from 12 to 35 systems but did not complete all required security processes and procedures (such as preparing system security plans) for many of the newly added systems.
- GAO’s incident response and handling procedures investigate security events, such as a denial of service attack, but deciding whether to classify such events as incidents—and, thus, to consider reporting them to other external organizations—needs additional management involvement.
- GAO has continued to make progress in establishing its privacy program and protecting personally identifiable information, but implementing additional requirements, such as providing annual privacy awareness training, would help further strengthen this program.

Recommendations: This report includes recommendations for GAO to (1) complete and document required information security processes and procedures for all systems in the systems inventory, (2) modify the agency’s incident handling and response procedures to increase Chief Information Officer involvement in the incident classification process to help ensure that security events are appropriately classified and reported, and (3) continue efforts to implement additional requirements for the agency’s privacy program. In commenting on a draft of the report, GAO concurred with these recommendations and described actions it is undertaking to address them.