September 2013

FEDERAL INFORMATION SECURITY

Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness

GAO Highlights

Highlights of GAO-13-776, a report to congressional committees

Why GAO Did This Study

FISMA requires the Comptroller General to periodically report to Congress on agency implementation of the act's provisions. To this end, this report summarizes GAO's evaluation of the extent to which agencies have implemented the requirements of FISMA, including the adequacy and effectiveness of agency information security policies and practices. To do this, GAO analyzed its previous information security reports, annual FISMA reports and other reports from the 24 major federal agencies, reports from inspectors general, and OMB's annual reports to Congress on FISMA implementation. GAO also interviewed agency officials at OMB, DHS, NIST, and 6 agencies selected using the total number of systems the agencies reported in fiscal year 2011.

What GAO Recommends

GAO and inspectors general have previously made numerous recommendations to improve agencies' information security programs. The agencies generally agreed with GAO's recommendations. In addition, GAO previously recommended that OMB revise annual reporting guidance to require performance targets to which OMB generally agreed. GAO is also recommending that the Director of OMB ensure that metrics are incorporated that assess the effectiveness of information security programs in OMB's annual FISMA reporting instructions to agencies and inspectors general.

View GAO-13-776. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

In fiscal year 2012, 24 major federal agencies had established many of the components of an information security program required by The Federal Information Security Management Act of 2002 (FISMA); however, they had partially established others. FISMA requires each federal agency to establish an information security program that incorporates eight key components, and each agency inspector general to annually evaluate and report on the information security program and practices of the agency. The act also requires the Office of Management and Budget (OMB) to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies and the National Institute of Standards and Technology to develop security standards and guidelines. The table below shows agency implementation of information security program components in fiscal year 2012.

Agency Implementation of Information Security Program Components in Fiscal Year 2012

	Number of agencies	
Program components	**Fully implemented**	**Partially implemented**
Establishing a program for managing information security risk	18	6
Documenting policies and procedures	10	12[a]
Selecting security controls for systems	18	6
Establishing a security training program	22	2
Monitoring controls on an ongoing basis	13	10[b]
Establishing a remediation program	19	5
Establishing an incident response and reporting program	20	3[b]
Establishing a continuity of operations program	18	5[b]

Source: GAO analysis of agency and inspector general data.

[a]An additional two agencies did not fully evaluate this program component in fiscal year 2012.

[b]One additional agency did not fully evaluate this program component in fiscal year 2012.

The extent to which agencies implemented security program components showed mixed progress from fiscal year 2011 to fiscal year 2012. For example, according to inspectors general reports, the number of agencies that had analyzed, validated, and documented security incidents increased from 16 to 19, while the number able to track identified weaknesses declined from 20 to 15. GAO and inspectors general continue to identify weaknesses in elements of agencies' programs, such as the implementation of specific security controls. For instance, in fiscal year 2012, almost all (23 of 24) of the major federal agencies had weaknesses in the controls that are intended to limit or detect access to computer resources.

OMB and the Department of Homeland Security (DHS) continued to develop reporting metrics and assist agencies in improving their information security programs; however, the metrics do not evaluate all FISMA requirements, such as conducting risk assessments and developing security plans; are focused mainly on compliance rather than effectiveness of controls; and in many cases did not identify specific performance targets for determining levels of implementation. Enhancements to these metrics would provide additional insight into agency information security programs.