June 2014

INFORMATION SECURITY

Additional Oversight Needed to Improve Programs at Small Agencies

GAO Highlights

Highlights of GAO-14-344, a report to congressional requesters

Why GAO Did This Study

Small federal agencies—generally those with 6,000 or fewer employees—are, like larger agencies, at risk from threats to information systems that support their operations and the information they contain, which can include personally identifiably information. Federal law and policy require small agencies to meet information security and privacy requirements and assign responsibilities to OMB for overseeing agencies' activities. OMB has assigned several of these duties to DHS.

GAO was asked to review cybersecurity and privacy at small agencies. The objectives of this review were to determine the extent to which (1) small agencies are implementing federal information security and privacy laws and policies and (2) OMB and DHS are overseeing and assisting small agencies in implementing their information security and privacy programs. GAO selected six small agencies with varying characteristics for review; reviewed agency documents and selected systems; and interviewed agency, OMB, and DHS officials.

What GAO Recommends

GAO recommends that OMB report on all small agencies' implementation of security and privacy requirements. GAO also recommends that DHS develop services and guidance targeted to small agencies' environments. GAO is making recommendations to the six agencies reviewed to address their information security and privacy weaknesses in a separate, restricted report. OMB and DHS generally concurred with the recommendations.

View GAO-14-344. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

The six small agencies GAO reviewed have made mixed progress in implementing elements of information security and privacy programs as required by the Federal Information Security Management Act of 2002, the Privacy Act of 1974, the E-Government Act of 2002, and Office of Management and Budget (OMB) guidance (see figure).

Agencies' Implementation of Information Security and Privacy Elements in Fiscal Year 2013

	Agency 1	Agency 2	Agency 3	Agency 4	Agency 5	Agency 6
Information Security						
Risk assessments	◐	◐	○	◐	○	◐
Policies & procedures	◐	◐	○	◐	○	◐
System security plans	◐	◐	○	◐	○	◐
Security training program	◐	◐	○	●	○	◐
Continuous monitoring of security controls	◐	◐	○	◐	○	◐
Remediation program	◐	◐	○	◐	○	◐
Incident response & reporting	◐	◐	○	◐	○	◐
Continuity of operations program	◐	◐	○	◐	○	◐
Privacy						
Issue system of records notices	●	◐	○	○	○	◐
Assign senior agency official for privacy	●	●	●	●	○	●
Conduct privacy impact assessments [a]	●	●	○	○	N/A	○

● Fully implemented ◐ Partially implemented ○ Did not implement

Source: GAO analysis of agency documentation. | GAO-14-344

[a]Agency 5 was not required to complete a privacy impact assessment.

In a separate report for limited official use only, GAO is providing specific details on the weaknesses in the six selected agencies' implementation of information security and privacy requirements.

OMB and the Department of Homeland Security (DHS) took steps to oversee and assist small agencies in implementing security and privacy requirements. For example, OMB and DHS instructed small agencies to report annually on a variety of metrics that are used to gauge implementation of information security programs and privacy requirements. In addition, OMB and DHS issued reporting guidance and provided assistance to all federal agencies on implementing security and privacy programs. However, 55 of 129 small agencies identified by OMB and DHS are not reporting on information security and privacy requirements. Further, the agencies in GAO's review have faced challenges in using the guidance and services offered. Until OMB and DHS oversee agencies' implementation of information security and privacy program requirements and provide additional assistance, small agencies will continue to face challenges in protecting their information and information systems.