August 2014

INFORMATION SECURITY

Agencies Need to Improve Oversight of Contractor Controls

GAO Highlights

Highlights of GAO-14-612, a report to congressional requesters

Why GAO Did This Study

Federal agencies often rely on contractors to operate computer systems and process information on their behalf. Federal law and policy require that agencies ensure that contractors adequately protect these systems and information.

GAO was asked to evaluate how well agencies oversee contractor-operated systems. The objectives of this report were to assess the extent to which (1) selected agencies oversee the security and privacy controls for systems that are operated by contractors on their behalf and (2) executive branch agencies with government-wide guidance and oversight responsibilities have taken steps to assist agencies in ensuring implementation of information security and privacy controls by such contractors. To do this, GAO selected six agencies based on their reported number of contractor-operated systems and two systems at each agency using a non-generalizable random sample for review, analyzed agency policies and procedures, and examined security and privacy-related artifacts for selected systems. GAO also interviewed agency officials, and reviewed federal guidance and evaluated agency FISMA submissions.

What GAO Recommends

GAO is recommending that five of the six selected agencies develop procedures for the oversight of contractors and that OMB clarify reporting instructions to agencies. The five agencies generally agreed with the recommendations and OMB did not provide any comments.

View GAO-14-612. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Although the six federal agencies that GAO reviewed (the Departments of Energy (DOE), Homeland Security (DHS), State, and Transportation (DOT), the Environmental Protection Agency (EPA) and the Office of Personnel Management (OPM)) generally established security and privacy requirements and planned for assessments to determine the effectiveness of contractor implementation of controls, five of the six agencies were inconsistent in overseeing the execution and review of those assessments, resulting in security lapses. For example, in one agency, testing did not discover that background checks of contractor employees were not conducted. The following table shows the degree of implementation of oversight activities at selected agencies.

GAO Evaluation of Agency Oversight of Selected Contractor-Operated Systems

	Establish requirements	Plan assessment	Execute assessment	Review assessment
DOE	●	◐	◐	◐
DHS	●	●	●	●
State	◐	◐	◐	◐
DOT	◐	●	◐	◐
EPA	●	●	●	◐
OPM	●	●	◐	●

Source: GAO analysis of agency data. | GAO 14 612

● Fully Implemented ◐ Partially Implemented ○ Not Implemented

A contributing reason for these shortfalls is that agencies had not documented procedures for officials to follow in order to effectively oversee contractor performance. Until these agencies develop, document, and implement specific procedures for overseeing contractors, they will have reduced assurance that the contractors are adequately securing and protecting agency information.

The Office of Management and Budget (OMB), the National Institute of Standards and Technology, and the General Services Administration have developed guidance to assist agencies in ensuring the implementation of security and privacy controls by their contractors. However, OMB guidance to agencies for categorizing and reporting on contractor-operated systems is not clear on when an agency should identify a system as contractor-operated and therefore agencies are interpreting the guidance differently. In fiscal year 2012, inspectors general from 9 of the 24 major agencies found data reliability issues with agencies' categorization of contractor-operated systems. Without accurate information on the number of contractor-operated systems, OMB assistance to agencies to help improve their cybersecurity posture will be limited and OMB's report to Congress on the implementation of the Federal Information Security Management Act (FISMA) is not complete.