April 2005

INFORMATION SECURITY

Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk

GAO
Accountability•Integrity•Reliability

Highlights

Highlights of GAO-05-362, a report to congressional requesters

Why GAO Did This Study

The federal government relies extensively on information technology services and systems provided by contractors. The Federal Information Security Management Act of 2002 (FISMA) requires agencies to establish information security programs that extend to contractors and other users of federal data and systems, such as grantees, state and local governments, and research and educational institutions.

GAO was asked to (1) describe the information security risks associated with contractors and users with privileged access to federal data and systems; (2) identify methods federal agencies use to ensure security of information and systems provided or used by contractors and other users with privileged access to federal data; and (3) determine what steps the administration is taking to ensure implementation and oversight of security of federal information and systems provided or used by contractors and other users with privileged access.

What GAO Recommends

GAO recommends that the Office of Management and Budget (OMB) ensure that the Federal Acquisition Regulation aligns with FISMA and that agencies develop contractor oversight policies We also recommend that the Commerce develop unified guidance. OMB and Commerce generally agreed with the results of this report.

www.gao.gov/cgi-bin/getrpt?GAO-05-362.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen (202) 512-3317 or wilshuseng@gao.gov.

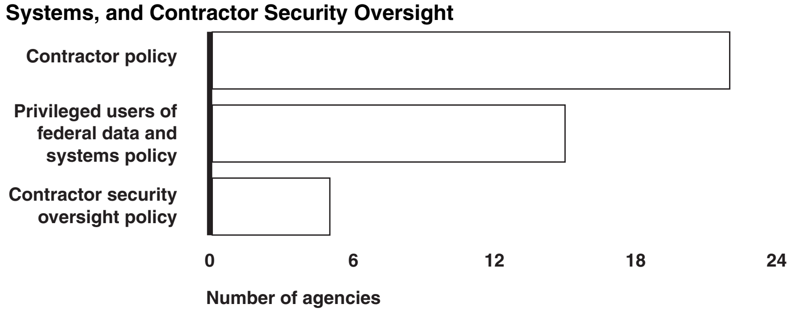
What GAO Found

Contractors and users with privileged access to federal data and systems provide valuable services that contribute to the efficient functioning of the government, but they present a range of related risks that must be managed effectively. Most agencies recognize risks to the confidentiality, integrity, and availability of their information and systems associated with the use of contractors and other users with privileged access to federal data and systems. In addition, agencies reported specific risks when contractors develop software or perform work at off-site facilities.

Agencies use contracts, policies, and self-assessments as methods to ensure information security oversight of contractors; however, each method has limitations and needs further strengthening. For example, most agencies have not incorporated FISMA requirements, such as annual testing of controls, into their contract language. Additionally, most of the 24 major agencies reported having policies for contractors and users with privileged access to federal data and systems; however, GAO's analysis of submitted agency policies found that only 5 agencies had established specific information security oversight policies (see figure). Finally, while the majority of agencies reported using a National Institute of Standards and Technology self-assessment tool to review contractor security capabilities, only 10 agencies reported using the tool to assess users with privileged access to federal data and systems, which may expose federal data to increased risk.

The administration continues in its efforts to improve information security oversight of contractors, but challenges remain. For example, efforts to update the Federal Acquisition Regulation to address information security have been under way since 2002, but are not complete. OMB continues to gather data about the number of agency systems, including those that are operated by contractors and how many have been reviewed. However, the submitted data showed that several agencies disagreed internally on the number of contractor or agency systems. Finally, federal agencies could benefit from unified guidance for overseeing information security of contractors and privileged users of federal data and systems.

Major Agencies with Security Policies for Contractors, Privileged Users of Federal Data and Systems, and Contractor Security Oversight



Source: GAO analysis based on agency data.