October 2006

INFORMATION SECURITY

Agencies Need to Develop and Implement Adequate Policies for Periodic Testing

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-65, a report to the Chairman, Committee on Government Reform, House of Representatives

Why GAO Did This Study

Agencies rely extensively on computerized information systems and electronic data to carry out their missions. To ensure the security of the information and information systems that support critical operations and infrastructure, federal law and policy require agencies to periodically test and evaluate the effectiveness of their information security controls at least annually.

GAO was asked to evaluate the extent to which agencies have adequately designed and effectively implemented policies for testing and evaluating their information security controls.

GAO surveyed 24 major federal agencies and analyzed their policies to determine whether the policies address important elements for periodic testing. GAO also examined testing documentation at 6 agencies to assess the quality and effectiveness of testing on 30 systems.

What GAO Recommends

This report contains recommendations to strengthen governmentwide guidance and reporting on agencies' periodic testing of information security controls. OMB said it would consider GAO's recommendations. The Department of Commerce stated that the National Institute of Standards and Technology is reviewing its guidance to assist agencies in strengthening their programs.

www.gao.gov/cgi-bin/getrpt?GAO-07-65.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal agencies have not adequately designed and effectively implemented policies for periodically testing and evaluating information security controls. Agencies' policies often did not include important elements for performing effective testing. For example, none of the agencies' policies addressed how to determine the depth and breadth of testing according to risk. Also, agencies did not always address other important elements, including the identification and testing of security controls common to multiple systems, the definition of roles and responsibilities of personnel performing tests, and the frequency of periodic testing.

The six case study agencies did not effectively implement policies for periodically testing and evaluating information security controls for the 30 systems reviewed. The methods and practices for testing and evaluating controls at the six agencies were not adequate to ensure that assessments were consistent, of similar quality, and repeatable. For example, these agencies did not always sufficiently document their test methods and results, did not define the assessment methods to be used when evaluating security controls, did not test security controls as prescribed, and did not include previously reported remedial actions or weaknesses in their test plans to ensure they had been addressed (see table). As a result, agencies may not have reasonable assurance that controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the agency. In addition, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving the agencies' information and systems vulnerable to attack or compromise.

Systems with Testing Weaknesses

Insufficient testing documentation	Inadequately defined assessment method	Inadequate test of security control	Inadequately documented remedial actions in test plans
28	7	24	18

Source: GAO analysis of agency FY 2005 test results (management, operational, and technical controls) and test documentation.