November 2002

COMPUTER SECURITY

Progress Made, But Critical Federal Operations and Assets Remain at Risk

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-303T, a testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives.

Why GAO Did This Study

Protecting the computer systems that support our critical operations and infrastructures has never been more important because of the concern about attacks from individuals and groups with malicious intent, including terrorism. These concerns are well founded for a number of reasons, including the dramatic increases in reported computer security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks.

As with other large organizations, federal agencies rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, as well as to helping prevent data tampering, fraud, and inappropriate disclosure of sensitive information. At the subcommittee's request, GAO discussed its analysis of recent information security audits and evaluations at 24 major federal departments and agencies.

www.gao.gov/cgi-bin/getrpt?GAO-03-303T.

To view the full testimony, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

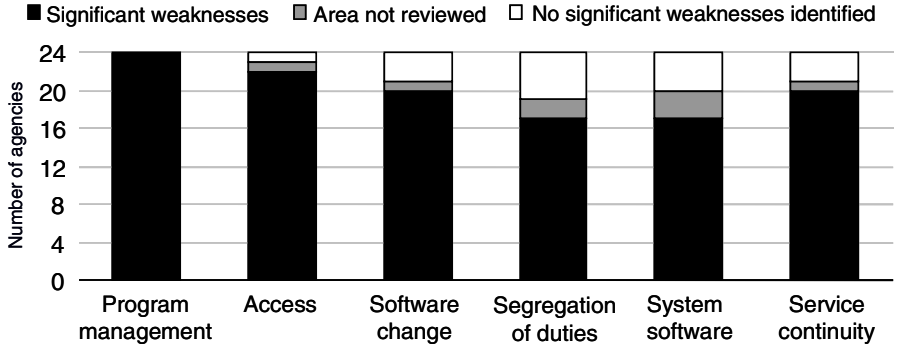
What GAO Found

Although GAO's current analyses of audit and evaluation reports for the 24 major departments and agencies issued from October 2001 to October 2002 indicate some individual agency improvements, overall they continue to highlight significant information security weaknesses that place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. GAO identified significant weaknesses in each of the 24 agencies in each of the six major areas of general controls. As in 2000 and 2001, weaknesses were most often identified in control areas for security program management and access controls. All 24 agencies had weaknesses in security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented (see figure below for list of major weaknesses).

Implementation of the Government Information Security Reform provisions ("GISRA") is proving to be a significant step in improving federal agencies' information security programs. It has also prompted the administration to take important actions to address information security, such as integrating security into the President's Management Agenda Scorecard. However, GISRA is scheduled to expire on November 29, 2002. GAO believes that continued authorization of such important information security legislation is essential to sustaining agencies' efforts to identify and correct significant weaknesses.

In addition to reauthorizing this legislation, there are a number of important steps that the administration and the agencies should take to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed. These steps include delineating the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection; providing more specific guidance on the controls agencies need to implement; obtaining adequate technical expertise to select, implement, and maintain controls to protect information systems; and allocating sufficient agency resources for information security.

Information Security Weaknesses at 24 Major Agencies



Source: Audit reports issued October 2001 through October 2002.