April 8, 2003

INFORMATION SECURITY

Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures

GAO Highlights

Highlights of GAO-03-564T, a testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives

Why GAO Did This Study

Protecting the computer systems that support federal agencies' operations and our nation's critical infrastructures—such as power distribution, telecommunications, water supply, and national defense—is a continuing concern. 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. GAO first designated computer security as high risk in 1997, and in 2003 expanded this high-risk area to include protecting the systems that support our nation's critical infrastructures, referred to as cyber critical infrastructure protection or cyber CIP.

GAO has made previous recommendations and periodically testified on federal information security weaknesses—including agencies' progress in implementing key legislative provisions on information security—and the challenges that the nation faces in protecting our nation's critical infrastructures. GAO was asked to provide an update on the status of federal information security and CIP.

www.gao.gov/cgi-bin/getrpt?GAO-03-564T.

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.

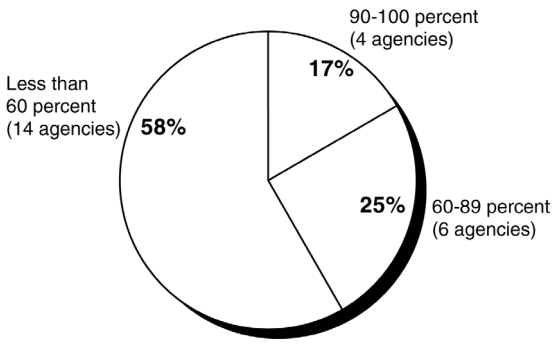
What GAO Found

With the enactment of the Federal Information Security Management Act of 2002, the Congress continued its efforts to improve federal information security by permanently authorizing and strengthening key information security requirements. The administration has also made progress through a number of efforts, among them the Office of Management and Budget's emphasis of information security in the budget process.

However, significant information security weaknesses at 24 major agencies continue to place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. Although recent reporting by these agencies showed some improvements, GAO found that agencies still have not established information security programs consistent with the legal requirements. For example, periodic testing of security controls is essential to security program management, but for fiscal year 2002, 14 agencies reported they had tested the controls of less than 60 percent of their systems (see figure below). Further information security improvement efforts are also needed at the governmentwide level, and these efforts need to be guided by a comprehensive strategy in which roles and responsibilities are clearly delineated, appropriate guidance is given, adequate technical expertise is obtained, and sufficient agency information security resources are allocated. Although improvements have been made in protecting our nation's critical infrastructures and continuing efforts are in progress, further efforts are needed to address critical challenges that GAO has identified over the last several years. These challenges include

- developing a comprehensive and coordinated national CIP plan;
- improving information sharing on threats and vulnerabilities between the private sector and the federal government, as well as within the government itself;
- improving analysis and warning capabilities for both cyber and physical threats; and
- encouraging entities outside the federal government to increase their CIP efforts.

Percentage of systems with security controls tested during fiscal year 2002



Source: Agency-reported data.