GAO
Accountability•Integrity•Reliability
Highlights

Highlights of GAO-03-1037T, a testimony before the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives

July 24, 2003

INFORMATION SECURITY

Further Efforts Needed to Fully Implement Statutory Requirements in DOD

Why GAO Did This Study

The Department of Defense (DOD) faces many risks in its use of globally networked computer systems to perform operational missions—such as identifying and tracking enemy targets—and daily management functions—such as paying soldiers and managing supplies. Weaknesses in these systems, if present, could give hackers and other unauthorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive military data.

GAO was asked, among other things, to discuss DOD's efforts to protect its information systems and networks from cyber attack, focusing on its reported progress in implementing statutory information security requirements.

www.gao.gov/cgi-bin/getrpt?GAO-03-1037T.

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

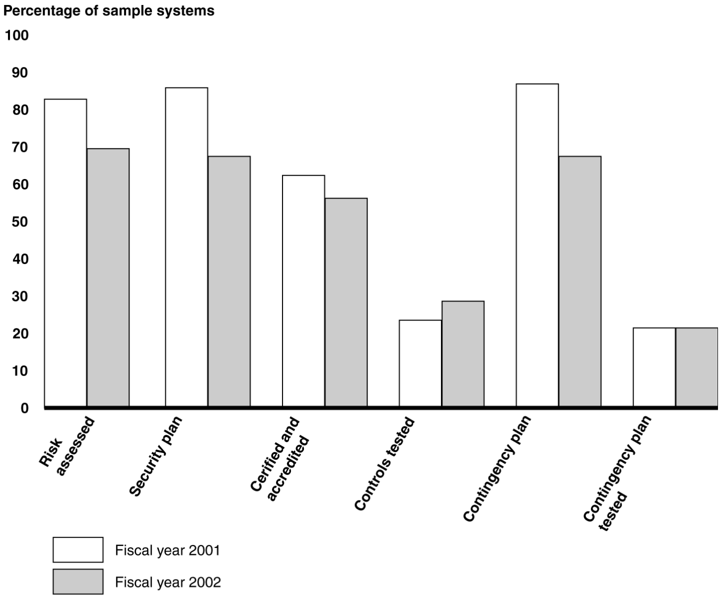
What GAO Found

In its fiscal year 2002 report on efforts to implement information security requirements under Government Information Security Reform law, DOD reported that it has an aggressive information assurance program and highlighted several initiatives to improve it. These initiatives included developing an overall strategy and issuing numerous departmentwide information security policy documents. DOD's reporting highlighted other accomplishments, but acknowledged that a number of challenges remain for the department in implementing both its policies and procedures and statutory information security requirements.

DOD reported several material control weaknesses, which included needing to decrease the time necessary for correcting reported weaknesses and ensuring that computer security policies are enforced and security capabilities are tested regularly. Further, performance data DOD reported for a sample of its systems showed that further efforts are needed to fully implement key information security requirements, such as testing systems' security controls, throughout the department (see figure).

Although DOD has undertaken its Defense-wide Information Assurance Program to promote integrated, comprehensive, and consistent practices across the department and has recently issued both policy guidance and implementation instructions, it does not have mechanisms in place for comprehensively measuring compliance with federal and Defense information security policies and ensuring that those policies are consistently practiced throughout DOD.

Reported Results for Selected DOD Information Security Performance Measures


Percentage of sample systems
Risk assessed
Security plan
Certified and accredited
Controls tested
Contingency plan
Contingency plan tested
Fiscal year 2001
Fiscal year 2002