March 2004

INFORMATION SECURITY

Technologies to Secure Federal Systems

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-467, a report to Congressional Requesters

Why GAO Did This Study

Federal agencies rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data is essential to preventing data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information.

Congress and the executive branch have taken actions to address this challenge, such as enacting and implementing the Federal Information Security Management Act (FISMA). FISMA and other federal guidance discuss the need for specific technical controls to secure information systems. In order to meet the requirements of FISMA to effectively implement these technical controls, it is critical that federal agencies consider whether they have adequately implemented available cybersecurity technologies.

GAO was asked by the Chairmen of the House Committee on Government Reform and its Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census to identify commercially available, state-of-the-practice cybersecurity technologies that federal agencies can use to defend their computer systems against cyber attacks.

www.gao.gov/cgi-bin/getrpt?GAO-04-467.

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

What GAO Found

Many cybersecurity technologies offered in today's marketplace can serve as safeguards and countermeasures to protect agencies' information technology infrastructures. To assist agencies in identifying and selecting such technologies, we have categorized specific technologies according to the control functionality they provide and described what the technologies do, how they work, and their reported effectiveness. The following table defines these five control categories:

Cybersecurity Control Categories

Control category	Control functionality
Access controls	Restrict the ability of unknown or unauthorized users to view or use information, hosts, or networks.
System integrity	Ensures that a system and its data are not illicitly modified or corrupted by malicious code.
Cryptography	Includes encryption of data during transmission and when stored on a system. Encryption is the process of transforming ordinary data into code form so that the information is accessible only to those who are authorized to have access.
Audit and monitoring	Help administrators to perform investigations during and after a cyber attack.
Configuration management and assurance	Help administrators view and change the security settings on their hosts and networks, verify the correctness of security settings, and maintain operations in a secure fashion under conditions of duress.

Source: GAO analysis.

We identified 18 technologies that are available within these categories, including smart tokens—which establish users' identities through an integrated circuit chip in a portable device such as a smart card or a time-synchronized token—and security event correlation tools—which monitor and document actions on network devices and analyze the actions to determine if an attack is ongoing or has occurred.

The selection and effective implementation of cybersecurity technologies require adequate consideration of a number of key factors, including:

- implementing technologies through a layered, defense-in-depth strategy;
- considering the agency's unique information technology infrastructure when selecting technologies;
- utilizing results of independent testing when assessing the technologies' capabilities;
- training staff on the secure implementation and utilization of these technologies; and
- ensuring that the technologies are securely configured.