June 2008

INFORMATION SECURITY

Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-525, a report to congressional requesters

Why GAO Did This Study

Many federal operations are supported by automated systems that may contain sensitive information such as national security information that, if lost or stolen, could be disclosed for improper purposes. Compromises of sensitive information at numerous federal agencies have raised concerns about the extent to which such information is vulnerable. The use of technological controls such as encryption—the process of changing plaintext into ciphertext—can help guard against the unauthorized disclosure of sensitive information.

GAO was asked to determine (1) how commercially available encryption technologies can help agencies protect sensitive information and reduce risks; (2) the federal laws, policies, and guidance for using encryption technologies; and (3) the extent to which agencies have implemented, or plan to implement, encryption technologies. To address these objectives, GAO identified and evaluated commercially available encryption technologies, reviewed relevant laws and guidance, and surveyed 24 major federal agencies.

What GAO Recommends

GAO is making recommendations to (1) the Director of the Office of Management and Budget (OMB) to clarify guidance and (2) selected agencies to strengthen practices for planning and implementing the use of encryption. In comments on a draft of this report, OMB and the agencies generally agreed with the recommendations.

To view the full product, including the scope and methodology, click on GAO-08-525. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Commercially available encryption technologies can help federal agencies protect sensitive information that is stored on mobile computers and devices (such as laptop computers, handheld devices such as personal digital assistants, and portable media such as flash drives and CD-ROMs) as well as information that is transmitted over wired or wireless networks by reducing the risks of its unauthorized disclosure and modification. For example, information stored in individual files, folders, or entire hard drives can be encrypted. Encryption technologies can also be used to establish secure communication paths for protecting data transmitted over networks. While many products to encrypt data exist, implementing them incorrectly—such as failing to properly configure the product, secure encryption keys, or train users—can result in a false sense of security and render data permanently inaccessible.

Key laws frame practices for information protection, while federal policies and guidance address the use of encryption. The Federal Information Security Management Act of 2002 mandates that agencies implement information security programs to protect agency information and systems. In addition, other laws provide guidance and direction for protecting specific types of information, including agency-specific information. For example, the Privacy Act of 1974 requires that agencies adequately protect personal information, and the Health Insurance Portability and Accountability Act of 1996 requires additional protections for sensitive health care information. The Office of Management and Budget has issued policy requiring federal agencies to encrypt all data on mobile computers and devices that carry agency data and use products that have been approved by the National Institute for Standards and Technology (NIST) cryptographic validation program. Further, NIST guidance recommends that agencies adequately plan for the selection, installation, configuration, and management of encryption technologies.

The extent to which 24 major federal agencies reported that they have implemented encryption and developed plans to implement encryption of sensitive information varied across agencies. From July through September 2007, the major agencies collectively reported that they had not yet installed encryption technology to protect sensitive information on about 70 percent of their laptop computers and handheld devices. Additionally, agencies reported uncertainty regarding the applicability of OMB's encryption requirements for mobile devices, specifically portable media. While all agencies have initiated efforts to deploy encryption technologies, none had documented comprehensive plans to guide encryption implementation activities such as installing and configuring appropriate technologies in accordance with federal guidelines, developing and documenting policies and procedures for managing encryption technologies, and training users. As a result federal information may remain at increased risk of unauthorized disclosure, loss, and modification.