INFORMATION SECURITY

Agencies Report Progress, but Sensitive Data Remain at Risk

What GAO Found

Federal agencies have recently reported a spate of security incidents that put sensitive data at risk. Personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby exposing those individuals to loss of privacy, identity theft, and financial crimes. The wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches underscores the need for improved security practices.

As illustrated by these security incidents, significant weaknesses in information security controls threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. Almost all of the major federal agencies had weaknesses in one or more areas of information security controls (see figure). Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. For example, agencies did not consistently identify and authenticate users to prevent unauthorized access, apply encryption to protect sensitive data on networks and portable devices, and restrict physical access to information assets. In addition, agencies did not always manage the configuration of network devices to prevent unauthorized access and ensure system integrity, such as patching key servers and workstations in a timely manner; assign incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction; and maintain or test continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs.

Nevertheless, federal agencies have continued to report steady progress in implementing certain information security requirements. However, IGs at several agencies sometimes disagreed with the agency's reported information and identified weaknesses in the processes used to implement these and other security program activities. Further, opportunities exist to enhance reporting under FISMA and the independent evaluations completed by IGs.