Environmental Protection Agency Needs to Resolve Weaknesses

What GAO Found
Although the Environmental Protection Agency (EPA) has taken steps to safeguard the information and systems that support its mission, security control weaknesses pervaded its systems and networks, thereby jeopardizing the agency’s ability to sufficiently protect the confidentiality, integrity, and availability of its information and systems. The agency did not fully implement access controls, which are designed to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Specifically, the agency did not always (1) enforce strong policies for identifying and authenticating users by, for example, requiring the use of complex (i.e., not easily guessed) passwords; (2) limit users’ access to systems to what was required for them to perform their official duties; (3) ensure that sensitive information, such as passwords for system administration, was encrypted so as not to be easily readable by unauthorized individuals; (4) keep logs of network activity or monitor key parts of its networks for possible security incidents; and (5) control physical access to its systems and information, such as controlling visitor access to computing equipment. In addition to weaknesses in access controls, EPA had mixed results in implementing other security controls. For example, EPA conducted appropriate background investigations for employees and contractors to ensure sufficient clearance requirements had been met before permitting access to information and information systems. However,

- EPA had not always securely configured network devices and updated operating system and database software with patches to protect against known vulnerabilities.
- EPA had not always ensured equipment used for sanitization and disposal of media was tested to verify correct performance.

An underlying reason for the control weaknesses is that EPA has not fully implemented a comprehensive information security program. Although EPA has established a framework for its security program, the agency has not yet fully implemented all elements of its program. Specifically, it did not always finalize policies and procedures to guide staff in effectively implementing controls; ensure that all personnel were given relevant security training to understand their roles and responsibilities; update system security plans to reflect current agency security control requirements; assess management, operational, and technical controls for agency systems at least annually and based on risk; and implement a corrective action process to track and manage all weaknesses when remedial actions were necessary. Sustained management oversight and monitoring are necessary for EPA to implement these key information security practices and controls. Until EPA fully implements a comprehensive security program, it will have limited assurance that its information and information systems are adequately protected against unauthorized access, use, disclosure, modification, disruption, or loss.