

Fed IT laws – overview for online security center

Laws	Description Of The Laws
Office of Management and Budget Circular A-130, Management of Federal Information Resources, Appendix III, "Security of Federal Automated Information Resources"	Establishes a minimum set of controls to be included in federal IT security programs.
Computer Security Act of 1987	This statute set the stage for protecting systems by codifying the requirement for Government-wide IT security planning and training.
Paperwork Reduction Act of 1995	The PRA established a comprehensive information resources management framework including security and subsumed the security responsibilities of the Computer Security Act of 1987.
Clinger-Cohen Act of 1996	This Act linked security to agency capital planning and budget processes, established agency CIOs, and re-codified the Computer Security Act of 1987.
Presidential Decision Directive 63, "Protecting America's Critical Infrastructures"	This directive specifies agency responsibilities for protecting the nation's infrastructure; assessing vulnerabilities of public and private sectors, and eliminating vulnerabilities.
Presidential Decision Directive 67, "Enduring Constitutional Government and Continuity of Government"	Relates to ensuring constitutional government, continuity of operations (COOP) planning, and continuity of government (COG) operations.
OMB Memorandum 99-05, "Instructions on Complying with President's Memorandum of May 14, 1998, 'Privacy and Personal Information in Federal Records'"	This memorandum provides instructions to agencies on how to comply with the President's Memorandum of May 14, 1998 on "Privacy and Personal Information in Federal Records."
OMB Memorandum 99-18, "Privacy Policies on Federal Web Sites"	This memorandum directs Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing so.
OMB Memorandum 00-13, "Privacy Policies and Data Collection on Federal Web Sites"	The purpose of this memorandum is a reminder that each agency is required by law and policy to establish clear privacy policies for its Web activities and to comply with those policies.
General Accounting Office Federal Information System Control Audit Manual (FISCAM)	The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.
NIST Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems	This publication guides organizations on the types of controls, objectives, and procedures that comprise an effective Security Program.
NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems	This publication details the specific controls that should be documented in a Security Plan.
Federal Information Processing Standards	These documents (FIPS 31–196) contain legislative and executive mandates for improving the utilization and management of computers and IT systems in the federal government.

Figure 1: IT Security Framework Source of Controls Criteria