CMS Information Security Levels

System owners must determine the appropriate system security level based on the confidentiality, integrity and availability of the information, as well as its criticality to the agency's business mission. This is the basis for assessing the risks to CMS operations and assets and in selecting appropriate security controls and techniques.

CMS Standard for Information Security Levels establishes common criteria for security levels by information category. The first table defines the information security levels. The second table lists security levels for the various information categories. (Note: that mission critical information is its own category). In other words, the system owner locates his information category to find the appropriate system security level. In the cases where information of varying security levels are combined, the highest security level takes precedence. Where system availability or data integrity are of high importance, see the table footnote.

Information Security Levels

Security Level	Description	Explanation
Low	Moderately serious	• Noticeable impact on an agency's missions, functions, image, or reputation. A breach of this security level would result in a negative outcome; or • Would result in DAMAGE, requiring repairs, to an asset or resource.
Moderate	Very serious	• Severe impairment to an agency's missions, functions, image, and reputation. The impact would place an agency at a significant disadvantage; or • Would result in MAJOR damage, requiring extensive repairs to assets or resources.
High	Catastrophic	• Complete loss of mission capability for an extended period; or • Would result in the loss of MAJOR assets or resources and could pose a threat to human life.

Information Security Levels by Information Categories

Information Category	Explanation and Examples	System Security Level*
Investigation, intelligence-related, and security information (14 CFR PART 191.5(D))	Information related to investigations for law enforcement purposes; intelligence-related information that cannot be classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements.	High
Mission-critical information	Information designated as critical to an agency mission, includes vital statistics information for emergency operations.	High
Life-critical information	Information critical to life-support systems (i.e., information where inaccuracy, loss, or alteration could result in loss of life).	High

Information Security Levels by Information Categories (con't)

Information about persons	Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history).	Moderate
Financial, budgetary, commercial, proprietary and trade secret information	Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payroll, automated decision making, procurement, inventory, other financially-related systems, and site operating and security expenditures.	Moderate
Internal administration	Information related to the internal administration of an agency. Includes personnel rules, bargaining positions, and advance information concerning procurement actions.	Moderate
Other Federal agency information	Information, the protection of which is required by statute, or which has come from another Federal agency and requires release approval by the originating agency.	Moderate
New technology or controlled scientific information	Information related to new technology; scientific information that is prohibited from disclosure to certain foreign governments or that may require an export license from the Department of State and/or the Department of Commerce.	Moderate
Operational information	Information that requires protection during operations; usually time-critical information.	Moderate
System configuration management information	Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at an agency; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information.	Moderate
Public information	Any information that is declared for public consumption by official authorities. This includes information contained in press releases approved by the Office of Public Affairs or other official sources. It also includes Information placed on public access world-wide-web (WWW) servers.	Low
Other sensitive information	Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare.	Low

*This level is based on data sensitivity requirements for the information system. The low system security level may be increased to moderate (not to high) if the information system has significant integrity and/or availability requirements. The moderate level cannot be increased to high.