CMS System Security Levels by Information Type

CMS has defined eleven information types processed by CMS information systems. For each information type, CMS has used FIPS Publication 199, February 2004, *Standards for Security Categorization of Federal Information and Information Systems,* to determine its associated security category by evaluating the potential impact value, e.g. High, Moderate or Low, for each of the three security objectives, namely, confidentiality, integrity and availability. The resultant security categorization is the CMS System Security Level. This is the basis for assessing the risks to CMS operations and assets and in selecting appropriate security controls and techniques.

The first table defines the three system security levels. The second table lists FIPS 199 security levels for the various information types. The system security level for a FISMA system or application system is determined by its information type(s). NOTE: In the cases where information of varying security levels is combined in a FISMA system or application, the highest security level takes precedence.

System Security Level Definitions

Security Level	Result	Explanation
High (H)	Catastrophic Adverse Effect	• Severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; • Major damage to organizational assets; • Major financial loss; or • Severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Moderate (M)	Serious Adverse Effect	• Significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; • Significant damage to organizational assets; • Significant financial loss; or • Significant harm to individuals that does not involve loss of life or serious life threatening injuries
Low (L)	Limited Adverse Effect	• Degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; • Minor damage to organizational assets; • Minor financial loss; or Minor harm to individuals.

FIPS 199 Security Levels by Information Type

Information Types (Security Category [SC])	Explanation and Examples	System Security Level Security Categorization
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** SC = {(confidentiality, **H**), (integrity, **H**), (availability, **M**)}

Mission-critical information	Information and associated infrastructure directly involved in making payments for Medicare Fee-for-Service (FFS), Medicaid and State Children's Health Insurance Program (SCHIP).	**HIGH** SC = {(confidentiality, **H**), (integrity, **H**), (availability, **H**)}
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), Equal Employment Opportunity (EEO), personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history as well as personally identifiable information (PII), individually identifiable information (IIF), or personal health information (PHI) covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).	**MODERATE** SC = {(confidentiality, **M**), (integrity, **M**), (availability, **M**)}
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 payments, payroll, automated decision making, procurement, market-sensitive, inventory, other financially-related systems, and site operating and security expenditures.	**MODERATE** SC = {(confidentiality, **M**), (integrity, **M**), (availability, **M**)}
Internal administration	Information related to the internal administration of an agency. Includes personnel rules, bargaining positions, advance information concerning procurement actions, management reporting, etc.	**MODERATE** SC = {(confidentiality, **M**), (integrity, **M**), (availability, **M**)}
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** SC = {(confidentiality, **M**), (integrity, **M**), (availability, **L**)}
New technology or controlled scientific information	Information related to new technology; scientific information that is prohibited from disclosure or that may require an export license from the Department of State and/or the Department of Commerce.	**MODERATE** SC = {(confidentiality, **M**), (integrity, **M**), (availability, **L**)}
Operational information	Information that requires protection during operations; usually time-critical information.	**MODERATE** SC = {(confidentiality, **M**), (integrity, **M**), (availability, **M**)}
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** SC = {(confidentiality, **M**), (integrity, **M**), (availability, **M**)}
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** SC = {(confidentiality, **L**), (integrity, **L**), (availability, **L**)}
Public information	Any information that is declared for public consumption by official authorities and has no identified requirement for integrity or availability. This includes information contained in press releases approved by the Office of Public Affairs or other official sources.	**LOW** SC = {(confidentiality, **L**), (integrity, **L**), (availability, **L**)}