CMS System Security and e-Authentication Assurance Levels by Information Type

This document establishes the system security levels and electronic authentication (e-Authentication) assurance levels for the information and information systems that support the operations and assets of CMS, including those provided or managed by another agency, contractor, or other source.

1. Security Objectives

The Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347, and Federal Information Processing Standard (FIPS) Publication 199, February 2004, *Standards for Security Categorization of Federal Information and Information Systems*, define three (3) security objectives for information and information systems. Table 1 lists these three (3) security objectives and their FISMA and FIPS 199 definitions.

Table 1 Information and Information System Security Objectives

Security Objectives	FISMA Definition [44 U.S.C., Sec. 3542]	FIPS 199 Definition
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"	A loss of *confidentiality* is the unauthorized disclosure of information.
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"	A loss of *integrity* is the unauthorized modification or destruction of information.
Availability	"Ensuring timely and reliable access to and use of information…"	A loss of *availability* is the disruption of access to or use of information or an information system.

2. Potential Impact Levels

FIPS 199 also defines three (3) levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability [CIA]). The application of the FIPS 199 definitions takes place within the context of each organization and the overall national interest. Table 2 lists the three (3) FIPS 199 potential impact levels and their definition.

Table 2 Potential Impact Levels and Definitions

Security Level	Result	Explanation
High (H)	Severe or 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.

In FIPS 199, the security category of an information type can be associated with both user information and system information, and can be applicable to information in either electronic or non-electronic form. It is also used as input in considering the appropriate security category for a system. Establishing an appropriate security category for an information type requires determining the potential impact for each security objective associated with the particular information type. The generalized format for expressing the security category (SC) of an information type is:

SC information system = {(confidentiality impact), (integrity impact), (availability impact)}, where the acceptable values for potential impact are High, Moderate, or Low.

3. e-Authentication Assurance Level

Office of Management and Budget (OMB) Memorandum 04-04, December 16, 2003, *E-Authentication Guidelines for Federal Agencies,* defines four (4) levels of authentication (i.e., Levels 1−4) required by all Federal agencies for electronic government transactions[1]. E-Authentication is the process of establishing confidence in user identities electronically presented to an information system. Although not all electronic transactions require authentication, e-Authentication applies to all such transactions for which authentication is required. Note that, for the purposes of e-authentication, the authentication requirements apply to *users accessing the applicable data described*. If the system does not (or cannot) present the described information to the user, then that category does not apply, even though the data may exist within the system.

OMB defines the required level of authentication assurance (i.e., e-Authentication) in terms of the likely consequences of an authentication error. Each assurance level describes the degree of

[1] OMB M-04-04 defines a transaction as: a discrete event between user and systems that supports a business or programmatic purpose.

certainty that the user has presented an identifier (i.e., a credential[2]) that refers to his/her identity. In this context, assurance is defined as: (i) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and (ii) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table 3 lists the four (4) OMB e-Authentication assurance levels and describes their degree of authentication confidence.

Table 3 e-Authentication Assurance Level Definitions

e-Authentication Assurance Level	Definition
Level 1	Little or no confidence in the asserted identity's validity.
Level 2	Some confidence in the asserted identity's validity.
Level 3	High confidence in the asserted identity's validity.
Level 4	Very high confidence in the asserted identity's validity.

Table 4 lists the four (4) e-Authentication assurance levels and describes the degree of authentication, cryptography, and identity proofing required for each level. As the consequences of an authentication error become more serious, the required level of assurance increases.

Table 4 e-Authentication Assurance Level Requirements

e-Authentication Assurance Level	e-Authentication Requirement
Level 1	• Requires the claimant prove, through a secure authentication protocol that he or she controls a single authentication factor to provide some assurance that the same claimant (who may be anonymous) is accessing the protected transaction. • Little or no confidence exists in the asserted identity. • Cryptography is not required to block offline attacks by an eavesdropper. • No identity proofing is required.
Level 2	• Requires the claimant prove, through a secure authentication protocol that he or she controls a single authentication factor. • Confidence exists that the asserted identity is accurate. • Approved cryptography is required to prevent eavesdroppers. • Identity proofing procedures require presentation of identifying materials or information.
Level 3	• Requires the claimant prove through a cryptographic protocol that he or she controls a minimum of two authentication factors (i.e., multi-factor). Three kinds of tokens may be used: "soft" cryptographic tokens, "hard" cryptographic tokens, and "one-time password" device tokens. The claimant must unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two-factor authentication. • High confidence exists that the asserted identity is accurate. • Approved cryptography is required for all operations. • Identity proofing procedures require verification of identifying materials and information.

[2] A credential is defined as: an object that is verified when presented to the verifier in an authentication transaction.

e-Authentication Assurance Level	e-Authentication Requirement
Level 4	• Requires the claimant prove through a cryptographic protocol that he or she controls a minimum of two authentication factors but only "hard" cryptographic tokens are allowed. • Very high confidence exists that the asserted identity is accurate. • Strong, approved cryptographic techniques are used for all operations. • Requires in-person appearance and identity proofing by verification of two independent ID documents or accounts, one of which must be current primary Government picture ID that contains applicant's picture, and either address of record or nationality (e.g., driver's license or passport), and a new recording of a biometric of the applicant.

The e-Authentication assurance level is determined by assessing the potential risks to CMS and by identifying measures to minimize their impact. The risks from an authentication error are a function of two factors: (i) potential harm or impact, and (ii) the likelihood of such harm or impact, as they apply to six (6) OMB-defined potential impact categories. The potential impact for each of the potential impact categories is assessed using the potential impact values described in FIPS 199 (i.e., High, Moderate, or Low).

The assurance level is determined by comparing the potential impact category to the potential impact value associated with each assurance level, as shown in Table 5. The required assurance level is determined by locating the highest level whose impact profile meets or exceeds the potential impact for every impact category.

Table 5 Maximum Assurance Level for each Potential Impact Category

	Assurance Level Impact Profiles			
Potential Impact Categories	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod/High
Civil or criminal violations	N/A	Low	Mod	High

4. CMS System Security Levels and e-Authentication Assurance Levels

CMS has defined eleven (11) information types processed on or by CMS information systems. For each information type, CMS used FIPS 199 to determine its associated security category by evaluating the potential impact value (i.e., High, Moderate, or Low) for each of the three (3) FISMA/FIPS 199 security objectives (i.e., confidentiality, integrity and availability [CIA]). For each information type, CMS also used OMB M-04-04 to determine its e-Authentication assurance level (i.e., Levels 1−4) by evaluating the degree of authentication confidence required to protect the information.

The results of these determinations, which apply to all CMS information and information systems, are presented in Table 6. The CMS security levels in Table 6 are the basis for assessing the risks to CMS operations and assets, and in selecting the appropriate minimum security requirements in the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS), CMS*

Minimum Security Requirements (CMSR) standard. The e-Authentication levels in Table 6 are the basis for selecting the appropriate OMB M-04-04 e-Authentication assurance level.

Note: In cases where information of varying security levels is combined in a FISMA system or application, the highest security level takes precedence.

Table 6 FIPS 199 Security Levels/OMB M-04-04 e-Authentication Levels by CMS Information Type

Information Type	Explanation and Examples	System Security Level	e-Authentication 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** SC = {(confidentiality, **H**), (integrity, **H**), (availability, **M**)}	**Level 4**
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**)}	**Level 4**
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)}	**Case 1: A user can ONLY access or update information about themselves:** **Level 2** **Case 2: A user can ONLY submit, review, or update information about persons that THEY have provided DURING THE CURRENT SESSION:** **Level 2** **Case 3: A user, not covered in Cases 1 or 2, can access or update information about persons OTHER THAN themselves:** **Level 3**
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**)}	**Level 3**

Information Type	Explanation and Examples	System Security Level	e-Authentication Level
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**)}	**Level 3**
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**)}	**Level 3**
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**)}	**Level 3**
Operational information	Information that requires protection during operations; usually time-critical information.	**MODERATE** SC = {(confidentiality, **M**), (integrity, **M**), (availability, **M**)}	**Level 3**
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**)}	**Level 3**
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**)}	**Level 2**
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**)}	**Case 1: No tracking or control on a user-level basis is desired.** **Level 0** **(No authentication required)** **Case 2: Tracking or control on a user-level basis is desired for business purposes.** **Level 1**

C. Ryan Brewer
CMS Chief Information Security Officer and
Director, Office of the Chief Information Security Officer