Defense Health Agency

ADMINISTRATIVE INSTRUCTION

NUMBER 77
May 28, 2015

HIT/CSD

SUBJECT: Security Categorization (SC) and Control Selection for Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This Defense Health Agency Administrative Instruction (DHA-AI), based on the authority of References (a) and (b), and in accordance with (IAW) the guidance of References (c) through (h), establishes the DHA's procedures for the SC and Control Selection for DHA IT.

2. APPLICABILITY. This AI applies to:

a. All DHA personnel, to include: assigned or attached Service members, federal civilians, contractors (when required by the terms of the applicable contract), and other personnel assigned temporary, or permanent duties at DHA to include regional and field activities (remote locations).

b. DHA-owned IT or DHA-controlled IT that receives, processes, stores, displays, or transmits Department of Defense (DoD) information.

3. POLICY.

a. It is DHA policy, IAW Reference (e), that the categorization and control selection of DHA IT will be a coordinated effort between the Program Manager (PM)/System Manager (SM), Information System Owner (ISO), Information Owner (IO), Mission Owner(s), Information System Security Manager (ISSM), and Authorizing Official (AO).

b. DHA Systems storing, transmitting, processing, displaying, or having unfettered access to Personally Identifiable Information (PII) or Protected Health Information (PHI) will be categorized, at a minimum, as follows: (confidentiality, Moderate), (integrity, Moderate), (availability, Moderate).

4. RESPONSIBILITIES. See Enclosure 2

5. PROCEDURES. SC of DHA IT is a three-step process in which:

a. The information type is identified.

b. The potential impact values for the information type(s) processed, stored, or transmitted by the system are determined (Enclosure 3).

c. The IT (Information Systems, Platform IT, IT Service, or IT Product) is categorized (Enclosure 4).

The Risk Management Framework (RMF) Knowledge Service (KS) and enterprise Mission Assurance Support Service (eMASS) provide tools to support security control selection based on the SC.

6. RELEASABILITY. **Not cleared for public release**. This AI is available to DHA employees and contractor support personnel with Common Access Card authorization on the DHA Intranet.

7. EFFECTIVE DATE. This DHA AI:

a. Is effective upon signature.

b. Will expire 10 years from the date of signature if it has not been reissued or cancelled before this date IAW DoD Instruction 5025 (Reference (c)).

Douglas J. Robb, DO, MPH
Lieutenant General, USAF, MC, CFS
Director

Enclosures:
1. References
2. Responsibilities
3. Security Categorization of Information
4. Security Categorization of IT
Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013

(b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013

(c) DoD Instruction 5025, "DoD Issuances Program," June 6, 2014, as amended

(d) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014

(e) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

(f) Committee on National Security Systems Instruction No. 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014

(g) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Volume II, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008

(h) Privacy Act and Health Insurance Portability and Accountability Act of 1996

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, HEALTH INFORMATION TECHNOLOGY (HIT) DIRECTORATE. The Director, HIT, IAW Reference (d), shall implement the DHA cybersecurity risk management process to protect DHA information and IT.

2. ISO/PM/SM AND IO. The ISO/PM/SM, IO, and Mission Owner(s), with the help of the ISSM, will categorize DHA IT, and the AO will approve the categorization.

a. The IO and the Mission Owner should refer to inputs from the System Development Life Cycle (SDLC) initiation phase, such as the concept of operations general descriptive information and functional and technical requirements specified for the system to assist in determining the information type. The level of the effort required to execute subsequent steps in the SDLC depends in part on the results of the SC. Systems with higher impact level designations require a greater number of security controls and control enhancements; security control implementation and assessment activities for those systems tend to take longer or require more resources.

b. The ISSM will support the PM, SM, ISO, IO, and Capabilities Manager in the determination of the SC by providing technical advice.

c. The IO and the Mission Owner will determine the SC of the information type (Enclosure 2) by:

(1) Assigning an impact value for confidentiality of High, Moderate, or Low.

(2) Assigning an impact value for integrity of High, Moderate, or Low.

(3) Assigning an impact value for availability of High, Moderate, or Low.

(4) Determining the requirement to include the security controls for PII or PHI in the Privacy Overlay Appendix F (Reference (f)).

d. The ISO/PM/SM will determine the SC of the information system (Enclosure 4) by:

(1) Assigning an impact value for confidentiality of High, Moderate, or Low.

(2) Assigning an impact value for integrity of High, Moderate, or Low.

(3) Assigning an impact value for availability of High, Moderate, or Low.

e. The IO and Mission Owner will coordinate with the ISO/PM/SM on the SC of the information type and information system to determine impact to the acquisition life cycle and to ensure the appropriate level of information security is designed into the IT solution.

f. AO. The AO will review the SC decision to ensure the appropriate level of information security is assigned to the information and designed into the IT.

3. ISO/PM/SM. The ISO/PM/SM will document the SC decision with supporting rationale as a required capability in the initial capabilities document, the capability development document, the capabilities production document, and the cybersecurity strategy within the program protection plan.

4. ISSM. The ISSM will document the SC decision with supporting rationale in the system security plan and the DHA initiation of the eMASS.

5. ISSM. The ISSM will select the security controls IAW Reference (f) and the implementation values from the RMF KS (Reference (e)).

6. ISSM. The ISSM will ensure the security controls are populated in the system registration in the eMASS.

ENCLOSURE 3

SECURITY CATEGORIZATION OF INFORMATION

1. DoD. DoD, in utilizing Reference (f) for SC, has aligned with the national security community and the other executive agencies of the Federal Government for mapping types of information and information systems to security categories (confidentiality, availability, and integrity). Categorization guidance is intended to ensure that information is protected by security controls commensurate with sensitivity of the information. Reference (f) directs the use of information types contained in Reference (g). The information types, identified in paragraph 3 of this enclosure, are most relevant to the DHA. NIST SP 800-60 Volume II provides additional reference types for consideration.

2. DHA. DHA programs and activities are responsible for ensuring and providing for the health and well-being of DoD's beneficiaries through the delivery of IT capabilities. This IT supports the direct provision of health care services, as well as the monitoring and tracking of indicators for the detection of trends and identification of illnesses/diseases. Some information associated with health care involves confidential patient information (PII or PHI), subject to Reference (h). The following factors should be considered with respect to security impacts for each information type.

a. Each information type should be evaluated for confidentiality with respect to the impact level that would be realized with unauthorized disclosure of each known variant of the information belonging to the type and each use of the information by the system under review. For DHA IT storing, transmitting, processing, displaying, or having unfettered access to PII/PHI, confidentiality will, at a minimum, be set to "Moderate."

(1) Determine if a malicious adversary or a trusted user could use the unauthorized disclosure of information to do limited/serious/severe harm to agency operations, agency assets, or individuals.

(2) Determine how a malicious adversary or trusted user could use the unauthorized disclosure of information to gain control of agency assets that might result in unauthorized modification of information, destruction of information, or denial of system services that would result in limited/serious/severe harm to agency operations, agency assets, or individuals.

(3) Determine if unauthorized disclosure/dissemination of elements of the information type could violate laws, executive orders, or agency regulations.

b. Each information type should be evaluated for integrity with respect to the impact that would be realized with unauthorized modification or destruction of each known variant of the information belonging to the type and each use of the information by the system under review. For DHA IT storing, transmitting, processing, displaying, or having unfettered access to PII/PHI, integrity will, at a minimum, be set to "Moderate."

(1) Determine if a malicious adversary or trusted user can use the unauthorized modification or destruction of information to do limited/serious/severe harm to agency operations, agency assets, or individuals.

(2) Determine if unauthorized modification/destruction of elements of the information type could violate laws, executive orders, or agency regulations.

(3) The consequences of integrity compromise can be either direct (e.g., modification of patient information, or a medical alert) or indirect (e.g., facilitation of unauthorized access to beneficiary information or denial of access to information or information system services).

(4) Integrity compromises could result in the endangerment of human life or other severe consequences. The impact can be particularly severe in the case of time-critical information.

c. Each information type should be evaluated for availability with respect to the impact level associated with the disruption of access to or use of information of each known variant of the information belonging to the type and each use of the information by the system under review. For DHA IT storing, transmitting, processing, displaying, or having unfettered access to PII/PHI, availability will, at a minimum, be set to "Moderate."

(1) Determine if a malicious adversary could use the disruption of access to or use of information to do limited/serious/severe harm to agency operations, agency assets, or individuals.

(2) Determine if disruption of access to or use of elements of the information type could violate laws, executive orders, or agency regulations.

(3) For health information, the availability impact level also depends on how long the information remains unavailable.

(4) Undetected loss of availability can be catastrophic for health information (e.g., if a provider searches for a drug allergy record, and that information is unavailable due to a cyber-event, the provider may think there is not a drug allergy record, and prescribe a medicine to which the patient is allergic).

3. INFORMATION TYPES RELEVANT TO DHA.

a. Personal Identity and Authentication Information. Personal identity and authentication information includes that information necessary to ensure that all persons who are potentially entitled to receive any DoD benefit are enumerated and identified so that the DoD can have reasonable assurance that they are paying or communicating with the right beneficiary. This information includes an individual beneficiary's Social Security Number, name, date of birth, place of birth, parents' names, etc. The recommended SC for the personal identity and authentication information type is as follows: SC = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}.

b. Access to Care. Access to care focuses on the access to appropriate health care. This includes streamlining efforts to receive care; ensuring care is appropriate in terms of type, care, intensity, location, and availability; providing seamless access to health knowledge; enrolling providers; performing eligibility determination, and managing patient movement. The minimum SC for access to care information is as follows: SC = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}.

c. Health Care Administration. Health care administration information assures that DoD health care resources are expended effectively to ensure quality, safety, and efficiency. This includes managing health care quality, cost, workload, utilization, and fraud/abuse efforts. The minimum SC for health care administration information that contains PII/PHI is as follows: SC = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}.

(1) If the IO, Mission Owner, and the ISO/PM/SM determine that unauthorized modification or destruction of health care administration information can result in inappropriate allocation or deployment of health care services and possible loss of human life, then the recommended SC for health care administration is as follows: SC = {(confidentiality, Moderate), (integrity, High), (availability, Moderate)}.

(2) If the IO, Mission Owner, and the ISO/PM/SM determine that the information does not contain PII/PHI, then the recommended SC for health care administration is as follows: SC = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}.

d. Health Care Delivery Services. Health care delivery services provide and support the delivery of health care to its beneficiaries. This includes assessing health status, planning health services, ensuring quality of services and continuity of care, and managing clinical information and documentation. The minimum SC for health care delivery services information that contains PII/PHI is as follows: SC = {(confidentiality, Moderate), (integrity, High), (availability, Moderate)}.

(1) If the IO, Mission Owner, and the ISO/PM/SM determine that delays in the communication of specific situations may be life threatening, then the recommended SC for health care delivery services is as follows: SC = {(confidentiality, Moderate), (integrity, High), (availability, High)}.

(2) If the IO, Mission Owner, and the ISO/PM/SM determine that the information does not contain PII/PHI, then the recommended SC for health care delivery services is as follows: SC = {(confidentiality, Low), (integrity, High), (availability, Low)}.

e. Health Care Research and Practitioner Education. Health care research and practitioner education fosters advancement in health discovery and knowledge. This includes developing new strategies to handle diseases; promoting health knowledge advancement; identifying new means for delivery of services, methods, decision models and practices; making strides in quality improvement; managing clinical trials and research quality; and providing for practitioner education. The recommended SC for health care research and practitioner education information that is available for public release is as follows: SC = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}. If the IO, Mission Owner, and the ISO/PM/SM determine that the information contains PHI or PII, then the minimum SC for health care research and practitioner education is as follows: SC = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}.

f. Population Health Management and Beneficiary Safety. Population health management and beneficiary safety assess health indicators and consumer products as a means to protect and promote the health of the general population. This includes monitoring of health, health planning, and health management of humans, animals, animal products, and plants, as well as tracking the spread of diseases and pests. It also includes evaluation of consumer products, drugs, and foods to assess the potential risks and dangers; education of the consumer and the general population; and facilitation of health promotion and disease and injury prevention. The recommended SC for population health management and beneficiary safety information is as follows: SC = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}.

(1) If the IO, Mission Owner, and the ISO/PM/SM determine that destruction of the information may adversely affect mission, operations, beneficiary confidence and in such cases, unauthorized modification or destruction of information can result in loss of human life, then the recommended SC for population health management and beneficiary safety is as follows: SC = {(confidentiality, Low), (integrity, High), (availability, Low)}.

(2) If the IO, Mission Owner, and the ISO/PM/SM determine that delays in the dissemination of the information may result in loss of human life, then the recommended SC for population health management and beneficiary safety is as follows: SC = {(confidentiality, Low), (integrity, Moderate), (availability, High)}.

(3) If the IO, Mission Owner, and the ISO/PM/SM determine that the information contains PHI or PII, then the minimum SC for health care research and practitioner education is as follows: SC = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}.

g. Budget Execution. Budget execution involves day-to-day requisitions and obligations for agency expenditures, invoices, billing dispute resolution, reconciliation, service level agreements, and distributions of shared expenses. The recommended provisional SC for budget execution information is as follows: SC = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}.

(1) If the IO, Mission Owner, and the ISO/PM/SM determine that the aggregate, budget execution information can reveal capabilities and methods that DHA considers extremely sensitive, then the recommended SC for budget execution is as follows: SC = {(confidentiality, Moderate to High), (integrity, Moderate), (availability, Low)}.

(2) If the IO, Mission Owner, and the ISO/PM/SM determine that in the case of agreements or transactions involving large monetary values, asset losses, and damage to agency operations, the potential for serious loss of beneficiary confidence is high, then the recommended SC for budget execution is as follows: SC = {(confidentiality, Low), (integrity, Moderate to High), (availability, Low)}.

h. Enterprise Architecture. Enterprise architecture is an established process for describing the current state and defining the target state and transition strategy for an organization's people, processes, and technology. The recommended provisional SC for the enterprise architecture information type is as follows: SC = {(confidentiality, Low), (integrity, Low), (availability, Low)}.

(1) If the IO, Mission Owner, and the ISO/PM/SM determine that disclosure of some of the background information that supports development of the DHA enterprise architecture can reveal sensitive vulnerabilities, capabilities, or methods of national security activities, then the recommended SC for enterprise architecture is as follows: SC = {(confidentiality, Moderate to High), (integrity, Low), (availability, Low)}.

(2) If the IO, Mission Owner, and the ISO/PM/SM determine that unauthorized modification or destruction of information affecting external communications that contain enterprise architecture information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the DHA, then the recommended SC for enterprise architecture is as follows: SC = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}.

i. System Development. System development supports all activities associated with the in-house design and development of software applications. The recommended SC for the system development information type is as follows: SC = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}.

j. Lifecycle/Change Management. Lifecycle/change management involves the processes that facilitate a smooth evolution, composition, and workforce transition of the design and implementation of changes to agency resources such as assets, methodologies, systems, or procedures. The recommended SC for the lifecycle/change management information type is as follows: SC = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}.

k. System Maintenance. System maintenance supports all activities associated with the maintenance of software applications. The recommended SC for the system maintenance information type is as follows: SC = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}.

l. IT Infrastructure Maintenance. The IT infrastructure maintenance type represents a complex set of data elements that are used to secure the design, implementation, and maintenance of systems and networks. The security of each of these data elements is dependent on the security of the other data elements. Security compromise of one data element type will propagate to others. The recommended SC for the IT infrastructure maintenance information type is as follows: SC = {(confidentiality, Low), (integrity, Low), (availability, Low)}.

m. Information Security. IT security involves all functions pertaining to the securing of Federal data and systems through the creation and definition of security policies, procedures, and controls covering such services as identification, authentication, and non-repudiation. The recommended SC for the IT security information type is as follows: SC = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}.

n. System and Network Monitoring. System and network monitoring supports all activities related to the real-time monitoring of systems and networks for optimal performance. System and network monitoring describes the use of tools and observation to determine the performance and status of information systems and is closely tied to other Information and Technology Management sub-functions. System and network monitoring information type should be considered broadly to include an agency's network [performance, health, and status] and security operations [intrusion monitoring, auditing, etc.] support. The recommended SC for the system and network monitoring information type is as follows: SC = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}.

o. Goods Acquisition. Goods acquisition involves the procurement of physical goods, products, and capital assets to be used by the DHA. The recommended SC for the goods acquisition information type is as follows: SC = {(confidentiality, Low), (integrity, Low), (availability, Low)}. If the IO, Mission Owner, and the ISO/PM/SM determine that the information type supports a system that is Mission Critical or Mission Essential, then the confidentiality impact level would range from moderate to high, the integrity impact level would range from moderate or high, and the availability impact level would range from moderate to high.

p. Inventory Control. Inventory control refers to the tracking of information related to procured assets and resources with regards to quantity, quality, and location. The recommended SC for the inventory control information type is as follows: SC = {(confidentiality, Low), (integrity, Low), (availability, Low)}. If the IO, Mission Owner, and the ISO/PM/SM determine that information type supports a system that is Mission Critical or Mission Essential, then the confidentiality impact level would range from moderate to high, the integrity impact level would range from moderate or high, and the availability impact level would range from moderate to high.

q. Logistics Management. Logistics management involves the planning and tracking of personnel and their resources in relation to their availability and location. The recommended SC for the logistics management information type is as follows: SC = {(confidentiality, Low), (integrity, Low), (availability, Low). If the IO, Mission Owner, and the ISO/PM/SM determine that information type supports a system that is Mission Critical or Mission Essential, then the confidentiality impact level would range from moderate to high, the integrity impact level would range from moderate or high, and the availability impact level would range from moderate to high.

r. Services Acquisition. Services acquisition involves the oversight and/or management of contractors and service providers from the private sector. The recommended SC for the services acquisition information type is as follows: SC = {(confidentiality, Low), (integrity, Low), (availability, Low)}. If the IO, Mission Owner, and the ISO/PM/SM determine that the information type is proprietary and/or proposal information, then the confidentiality impact level would range from moderate to high, and the integrity impact level would range from moderate to high.

4. The following table summarizes the set of minimum and recommended SCs from paragraph 3.

Recommended Security Categorizations for DHA Information

Information Type	Primary Security Categorization	Alternate Security Categorizations
Personal Identity and Authentication Information	(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)	None
Access to Care	PII/PHI: (confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)	None
Health Care Administration	(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)	(confidentiality, Moderate), (integrity, High), (availability, Moderate) (confidentiality, Low), (integrity, Moderate), (availability, Low).
Health Care Delivery Services	(confidentiality, Moderate), (integrity, High), (availability, Moderate)	(confidentiality, Moderate), (integrity, High), (availability, High) (confidentiality, Low), (integrity, High), (availability, Low)
Health Care Research and Practitioner Education	(confidentiality, Low), (integrity, Moderate), (availability, Low)	(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}
Population Health Management and Beneficiary Safety	(confidentiality, Low), (integrity, Moderate), (availability, Low)}	(confidentiality, Low), (integrity, High), (availability, Low) (confidentiality, Low), (integrity, Moderate), (availability, High)
Budget Execution	(confidentiality, Low), (integrity, Moderate), (availability, Low)	(confidentiality, Moderate to High), (integrity, Moderate), (availability, Low) (confidentiality, Low), (integrity, Moderate to High), (availability, Low)

Enterprise Architecture	(confidentiality, Low), (integrity, Low), (availability, Low)	confidentiality, Moderate to High), (integrity, Low), (availability, Low) (confidentiality, Low), (integrity, Moderate, (availability, Low)
System Development	(confidentiality, Low), (integrity, Moderate), (availability, Low)	None
Lifecycle/Change Management	(confidentiality, Low), (integrity, Moderate), (availability, Low)	None
System Maintenance	(confidentiality, Low), (integrity, Moderate), (availability, Low)	None
IT Infrastructure Maintenance	(confidentiality, Low), (integrity, Low), (availability, Low)	None
Information Security	(confidentiality, Moderate), (integrity, Moderate), (availability, Low)	None
System and Network Monitoring	(confidentiality, Moderate), (integrity, Moderate), (availability, Low)	None
Goods Acquisition	(confidentiality, Low), (integrity, Low), (availability, Low)	None
Inventory Control	(confidentiality, Low), (integrity, Low), (availability, Low)	None
Logistics Management	(confidentiality, Low), (integrity, Low), (availability, Low)	None
Services Acquisition	(confidentiality, Low), (integrity, Low), (availability, Low)	None

ENCLOSURE 4

SECURITY CATEGORIZATION OF IT

1. Determining the SC of IT requires that the ISO/PM/SM consider the security categories of all information types resident on the IT. For IT, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) will be the highest values from among those security categories that have been determined for each type of information resident on the IT. The format for expressing the SC of an information system is: SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)}, where the acceptable values for potential impact are Low, Moderate, or High.

2. The following information should be taken into consideration by the PM/SM/IO when categorizing the IT.

a. The impact level for a system security category may be higher than any security objective impact level for any information type processed by the system. Consideration of the following issues should be addressed in determining the SC:

(1) Aggregation of large quantities of a single information type can reveal sensitive patterns and plans, or facilitate access to sensitive or critical systems. Aggregation of information of several different and seemingly innocuous types can have similar effects. The sensitivity of a given data element is likely to be greater in context than in isolation (e.g., association of an account number with the identity of an individual and/or institution). The system security objective impact levels may need to be adjusted to a higher level than would be indicated by the security impact levels associated with any individual information type in cases of aggregation.

(2) Indirect access should be considered in determining the impact levels. Access to a system might result in some form of access to other systems (e.g., over a network), the sensitivity and criticality attributes of all systems to which such indirect access can result needs to be considered. Loss of data integrity or availability can have catastrophic consequences.

(3) Either physical or logical destruction of major assets can result in very large expenditures to restore the assets and/or long periods of time for recovery. Permanent loss/unavailability of information system capabilities can seriously hamper agency operations and, where direct services to the DoD beneficiaries are involved, have a severe adverse effect on confidence in the DHA.

(4) Unauthorized modification or destruction of information affecting external communications (e.g., DHA public web pages, electronic mail) may adversely affect operations and/or public confidence in the DHA.

(5) Identify all DHA information systems interacting with DHA infrastructure systems to enable an enterprise wide security perspective.

b. The value of “not applicable” cannot be assigned to any security objective in the context of establishing a security category for an information system. This is in recognition that there is an impact on the loss of confidentiality, integrity, and availability for an information system due to the fundamental requirement to protect the system-level processing functions and information critical to the operation of the information system.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AO	Authorizing Official
DHA	Defense Health Agency
DoD	Department of Defense
eMASS	Enterprise Mission Assurance Support Service
IAW	in accordance with
IO	Information Owner
IT	Information Technology
ISO	Information System Owner
ISSM	Information System Security Manager
KS	Knowledge Service
PHI	Protected Health Information
PII	Personally Identifiable Information
PM/SM	Program Manager/System Manager
RMF	Risk Management Framework
SC	Security Categorization
SP	Special Publication

PART II. DEFINITIONS

availability. The property of being accessible and useable upon demand by an authorized entity. Ensuring timely and reliable access to and use of information.

confidentiality. The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

impact values. The three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).

Low Impact Value. The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

amplification. A limited adverse effect means that the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is noticeably reduced; (ii) result in minor damage to organizational, critical infrastructure, or national security assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Note: Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

Moderate Impact Value. The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

amplification. A serious adverse effect means that the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is significantly reduced; (ii) result in significant damage to organizational, critical infrastructure, or national security assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals exceeding mission expectations.

Note: There is an expectation of certain losses when performing particular missions. In this case, the harm exceeds those expectations.

High Impact Value. The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

amplification. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a 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; (ii) result in major damage to organizational, critical infrastructure, or national security assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals exceeding mission expectations.

Note: There is an expectation of certain losses when performing particular missions. In this case, the harm exceeds those expectations.

IO. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal. The DHA Capability Mangers and/or Information Managers (IM) are the IO(s).

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

ISO. Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an IS.

integrity. The property whereby an entity has not been modified in an unauthorized manner. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Mission-Critical Information System. A system that meets the definitions of "information system" and "national security system" in the Clinger-Cohen Act, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (The designation of mission critical will be made by a DoD Component Head, a Combatant Commander, or their designee. A financial management IT system will be considered a mission-critical IT system as defined by the Under Secretary of Defense (Comptroller) (USD(C)). A "Mission-Critical Information Technology System" has the same meaning as a "Mission-Critical Information System."

Mission-Essential Information System. A system that meets the definition of "information system" in Title 44, United States Code, Section 3502, that the acquiring DoD Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The designation of mission-essential will be made by a DoD Component Head, a Combatant Commander, or their designee. A financial management IT system will be considered a mission-essential IT system as defined by the USD(C).) A "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System."