Defense Health Agency

ADMINISTRATIVE INSTRUCTION

NUMBER 5200.02
October 6, 2020

DAD-A&M/ISD

SUBJECT: Information Security Program

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 the guidance of References (c) through (ab), establishes the Defense Health Agency's (DHA) procedures for the Information Security (INFOSEC) Program.

2. APPLICABILITY. This DHA-AI applies to:

a. DHA and DHA Components (i.e., markets and military medical treatment facilities under the administration, direction, and control of the DHA).

b. All DHA personnel to include assigned, attached, or detailed active duty, reserves, or National Guard personnel, federal civilians, contractors when required by the terms of the applicable contract, volunteers, and other personnel assigned temporary or permanent duties at DHA and DHA Components.

3. POLICY IMPLEMENTATION. It is DHA's policy, pursuant to References (d) through (ab) to:

a. Identify and protect classified and controlled unclassified information (CUI) in accordance with References (d) through (u).

b. Employ, maintain and enforce standards for safeguarding, storing, destroying, transmitting, and transporting classified information.

c. Actively promote and implement security education and training throughout the DHA.

d. Protect classified information and CUI from unauthorized disclosure by appropriately marking, disseminating, and destroying such information.

e. Transmit classified information and CUI through the Communications Security (COMSEC) measures and procedures set forth in this DHA-AI and in accordance with DoD policy issuances.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Not cleared for public release.** This DHA-AI is available to authorized users from the DHA SharePoint site at: https://info.health.mil/cos/admin/pubs/SitePages/Home.aspx.

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 in accordance with Reference (c).

8. FORMS

a. SF Form 312, “Classified Information Nondisclosure Agreement” is available at: https://www.opm.gov/forms/standard-forms/.

b. DD Form 2933, “National Language Service Corps (NLSC) Detailed Skills Self-Assessment” is available at: https://www.esd.whs.mil/Directives/forms/.

c. DD Form 254, "Department of Defense Contract Security Classification Specification" is available at: https://www.esd.whs.mil/Directives/forms/.

/S/
RONALD J. PLACE
LTG, MC, USA
Director

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013, as amended
(b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013
(c) DHA-Procedural Instruction 5025.01, "Publication System," August 24, 2018
(d) DoD Manual 5200.01-Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended
(e) DoD Manual 5200.01-Volume 2, "DoD Information Security Program: Marking of Information," February 24, 2012, as amended
(f) DoD Manual 5200.01-Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
(g) DoD Manual 5200.01-Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012, as amended
(h) DoD Manual 5220.22, "National Industrial Security Program Operating Manual," February 28, 2006, as amended
(i) DoD Manual 5105.21-Volume 1, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security," October 19, 2012, as amended
(j) DoD Manual 5105.21-Volume 2, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security," October 19, 2012, as amended
(k) DoD Manual 5105.21-Volume 3, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities," October 19, 2012, as amended
(l) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended
(m) DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017
(n) DoD Instruction 8523.01, "Communications Security (COMSEC)," April 22, 2008
(o) DoD Instruction 8560.01, "Communications Security (COMSEC) Monitoring and Information Assurance (IA)," October 9, 2007, as amended
(p) National Security Agency/Central Security Service (NSA/CSS) 3-16, "Control of COMSEC Material," April 8, 2016 as amended[1]
(q) Intelligence Community Policy Guidance 403.1, "(U) Criteria for Foreign Disclosure and Release of Classified National Intelligence," March 13, 2013
(r) Intelligence Community Directive (ICD) 703, "Protection of Classified National Intelligence, Including Sensitive Compartmented Information," June 21, 2013
(s) Code of Federal Regulations, Title 32, Part 2002

[1] This reference can be found on Secret Internet Protocol Router Network (SIPRNet) at: www.iad.nsa.smil.mil/resources/library/nsa_office_of_policy_section/pdf/NSA_CSS_MAN-3-16_080505.pdf. If SIPRNet access is not available, contact the DHA Special Security Office at dha.sso@mail.mil or 703-681-7243.

(t) Security Executive Agent Directive (SEAD) 2, "Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position," September 14, 2014
(u) U.S. Department of Agriculture Food Safety and Inspection Service FSIS Directive 2620.2, "Guidelines for Handling and Distributing Classified Documents," September 7, 2006
(v) Office of Management and Budget Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017
(w) DoD 5400.11-R, DoD Privacy Program, May 14, 2007
(x) DHA-PI 8140.01, "Acceptable Use of DHA IT," October 16, 2018
(y) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(z) DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015, as amended
(aa) DoD Instruction 5200.33, "Defense Courier Operations," June 30, 2011
(ab) DoD Instruction 5200.01, Volume 4 "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA, will:

a. Be responsible for overall implementation, oversight, and compliance involving all matters of the DHA INFOSEC Program.

b. Provide adequate funding, personnel, and other resources for compliance per Reference (j).

c. Designate the Senior Agency Official (SAO) in writing.

d. Adhere to CUI responsibilities identified in Reference (g).

2. DEPUTY ASSISTANT DIRECTOR (DAD), ADMINISTRATION AND MANAGEMENT/ SAO. The DAD, Administration and Management/SAO is responsible for the direction, administration, and oversight of the INFOSEC education and training program in accordance with this DHA-AI, and References (h) through (j) and (p). The SAO must:

a. Establish procedures to ensure prompt and appropriate management action is taken in cases of compromise of classified information and unauthorized disclosure of CUI, improper classification or designation of information, violation of the provisions of this DHA-AI and References (g), (s), and (t), and incidents that may put classified information and CUI at risk of unauthorized disclosure.

b. Review, approve, or decline, direct oversight of all DHA requests for one-time or short duration access to classified information.

c. Designate the following officials in writing:

(1) Senior Intelligence Official (SIO)

(a) SIO duties are considered the individual's additional duty assignment to their regular position.

(b) The SIO must be sensitive compartmented information (SCI) indoctrinated and the highest-ranking military or civilian charged with direct foreign intelligence missions, functions, or responsibilities of the DHA.

(c) The SIO will report to the SAO.

(2) Activity Security Manager (ASM)

(a) ASM duties are considered the individual's additional duty assignment to their regular position.

(b) The ASM will have sufficient delegated authority to ensure personnel adhere to program requirements, and their position within the organization must ensure their credibility and enable them to raise security issues.

(c) The ASM will report to the SIO and cannot function as the Special Security Official (SSO) unless designated by the cognizant SIO.

(3) Activity Top Secret Control Official (TSCO)

(a) TSCO duties are considered the individual's additional duty assignment to their regular position.

(b) The TSCO will report to the ASM and SSO.

d. Direct, administer and oversee DHA's INFOSEC Program to include classification, declassification, safeguarding, and security education and training programs.

e. Direct, administer, and oversee the disclosure of classified information to foreign governments and foreign persons, and coordinate exemptions and waivers.

f. Establish and maintain an ongoing self-inspection and assessment program with oversight to evaluate and assess the effectiveness and efficiency of the DHA implementation of the INFOSEC Program as it pertains to classified information.

g. Establish and maintain a security education and training program as required by References (d) through (k), and ensure DHA personnel receive security education and training appropriate to their responsibilities.

h. Advise the applicable DHA DADs who create, handle, or store sensitive and classified information to properly implement, manage, and oversee their directorate INFOSEC Program. Persons appointed to these positions must be provided training as stated in Reference (i) and this DHA-AI.

i. Develop and maintain the DHA’s security education and training program and will designate personnel, as necessary, to assist in carrying out this responsibility.

j. Establish procedures to prevent unauthorized persons from accessing classified and sensitive information.

k. Establish and maintain declassification programs and plans that meet the requirements of this DHA-AI and ensure necessary resources are applied to the review of information to ensure it is neither classified for longer than necessary nor declassified prematurely.

l. Develop and maintain an automated Security Incident Reporting Program and a comprehensive security database reflecting final adjudication and investigation of security incidents.

m. Adhere to CUI responsibilities identified in Reference (g).

3. CHIEF, ENTERPRISE SECURITY, THREAT MANAGEMENT, AND SAFETY (ESTMS)/SIO. The Chief, ESTMS/SIO, must:

a. Exercise overall responsibility and management for the DHA INFOSEC Program, which includes sensitive and classified information (except SCI).

b. Direct, administer, and oversee the DHA SCI Program, to include classification, declassification, safeguarding, and security education and training programs for effective implementation.

c. Designate the following officials in writing:

(1) SSO

(a) Responsible for the day-to-day security management, operation, implementation, use, and dissemination of SCI as an additional duty assignment. Such designation must be made for any activity accredited for and authorized to receive, use, and store SCI and shall be submitted in writing.

(b) The SSO/Contractor Special Security Officials (CSSO) will be accredited and authorized to receive, use, and store SCI material, be Top Secret (TS)/SCI indoctrinated, and appointed in writing by the SIO.

(2) CSSO

(a) May be a contractor under a valid DHA contract that supports the SSO with the day-to-day security management, operation, implementation, use, and dissemination of SCI.

(b) Be SCI indoctrinated and appointed in writing by the SIO.

d. Ensure personnel are provided CUI education and training.

e. Establish, manage, and conduct security awareness training and education programs to all personnel to ensure complete, common, and continuing understanding and application of SCI security.

f. Ensure personnel are trained to provide a basic understanding of the nature of sensitive information, classified information, CUI, and the proper protection of such information in their possession to include protection from unauthorized disclosure.

g. Establish, manage, and conduct training programs for SCI security officials to enable them to perform the duties and meet the requirements contained in the Reference (i), References (j) through (l), and this DHA-AI.

h. Develop specific implementation procedures as necessary for the protection of SCI material.

i. Administer and oversee, within their respective organizations, those aspects of the SCI security programs not delegated to the Defense Intelligence Agency.

j. Ensure CUI is properly handled during the entire life cycle. This includes ensuring information is appropriately identified, marked, stored, disseminated, disposed of, and accounted for, as well as provide guidance on the handling of security incidents to minimize adverse effects and ensure appropriate corrective action is taken.

k. Establish required Memorandum of Agreement with other organizations, as necessary, on SCI areas of responsibility, training, operational needs, support, and services.

l. Implement Standard Operating Procedures (SOP) as required for further definition and clarification of security responsibilities.

4. ASM. The ASM must:

a. Manage and implement the activity's INFOSEC Program, except for the SCI program portion, and ensure its visibility and effectiveness on behalf of the Director, DHA.

b. Ensure all subordinate personnel who perform security duties are properly trained prior to assuming duties.

c. Ensure appropriate delegation letters and training certifications are maintained and available when requested by appropriate authorities and submitted to the SSO.

d. Ensure compliance with the requirements of References (d) through (r) and this DHA-AI when access to classified information is provided to contractors at DHA facilities and locations in connection with a classified contract.

e. Ensure security incidents pertaining to classified information, including foreign government information, are reported, recorded, coordinated with the proper authorities, and, when necessary, investigate and ensure appropriate action is taken to mitigate damage and prevent recurrence. Ensure incidents involving the loss or compromise of classified information are immediately referred to the SSO.

f. Provide direction and guidance to staff who create, handle, or store classified information.

g. Develop a centralized location that INFOSEC personnel need to manage their programs and to share best practices and develop and implement an electronic security manager handbook.

h. Develop a written Activity Security Instruction that includes provisions for safeguarding classified information during emergency situations.

5. ACTIVITY TSCO. The Activity TSCO is responsible for the INFOSEC Programs TS and TS/SCI control of material, and ensures compliance, oversight, development, and implementation in accordance with References (d) and this DHA-AI. Responsibilities include the accounting for, receipt, custody, and disposition of TS materials. The Activity TSCO must:

a. Maintain documents and other physical media (e.g., disk drives and removable computer media), maintain a system of accountability (e.g., registry), to record the receipt, reproduction, transfer, transmission, downgrading, declassification, and destruction of TS information and other special types of classified information.

b. Ensure inventories of TS information are conducted annually or more frequently when directed by the Director, DHA; SIO; SAO; or ASM; and when circumstances warrant.

c. Develop, implement, and manage site-specific SOPs which will be submitted to ESTMS for review and approval prior to execution.

d. Ensures all TS materials are accounted for and properly transferred when custodians are relieved of their duties.

6. SSO/CSSO. The SSO/CSSO must:

a. Process, control, transmit, transport, secure, package, and safeguard TS/SCI material and information.

b. Serve as the official channel for certifying and receiving TS/SCI visitor clearance and access requests.

c. Maintain the System of Record to reflect all personnel under their cognizance.

d. Develop and implement SOPs. Submission of SOPs will be to ESTMS for review and approval prior to their execution.

7. SPECIAL SECURITY REPRESENTATIVE (SSR), CONTRACTOR SPECIAL SECURITY REPRESENTATIVE (CSSR). The SSR, CSSR must:

a. Perform duties as assigned by the SSO. A CSSR includes a contractor under a valid contract that requires a DD Form 254, be Secret indoctrinated, and supports the SSR and SSO.

b. Process, control, transmit, transport, secure, package, and safeguard Secret material and information at the local level.

c. Maintain the System of Record to reflect all personnel under their cognizance at the local level.

d. Develop and implement SOPs at the local level. Submission of SOPs will be to ESTMS for review and approval prior to their execution.

8. DHA PERSONNEL. DHA personnel will comply with the following:

a. Individuals with access to classified material will adhere to the guidelines outlined in Reference (d).

b. Individuals with access to SCI material will adhere to the guidelines identified in Reference (i).

ENCLOSURE 3

PROCEDURES

1. BACKGROUND. SOPs for each section of this Enclosure will be developed and implemented and detail procedures and processes for the INFOSEC Program. All SOP(s) must be submitted to the ESTMS Office for review and approval prior to execution.

2. EDUCATION AND TRAINING

a. Security Training. Security education and training is continuous rather than irregular. Briefing sessions, and other formal presentations will be supplemented with other information and promotional efforts to ensure continuous awareness and performance quality is maintained.

b. Additional Training. In support of References (d) through (g) and this DHA-AI, the Director, DHA, may direct additional training requirements.

c. Initial Orientation Training

(1) All DHA personnel will receive an INFOSEC Initial Orientation within 30 days of arrival.

(2) Individuals with specified duties in the INFOSEC Program, as identified in this Enclosure, will be provided security education and training commensurate with job responsibilities sufficient to permit effective performance of those duties.

(3) The education and training may be provided before, concurrent with, or not later than 30 days following and assuming those duties, unless otherwise specified.

(4) Personnel with access to sensitive, classified, CUI material, and systems will successfully complete an approved Cyber Awareness Training per References (y) and (z).

(5) Personnel who are authorized to have access to sensitive and classified information systems will receive training which addresses, at a minimum:

(a) Proper use of information systems for creating, using, storing, processing, or transmitting classified information;

(b) Requirement for and application of markings, including portion markings, to information in electronic formats (e.g., documents, e-mail, briefings, web-based information, databases, spreadsheets). Marking, handling, storage, transportation, and destruction of classified computer media (e.g., floppy disks, compact disks, digital versatile disks, removable hard drives), and procedures to be followed when using classified removable data storage media; and;

(c) Procedures to be followed if an individual believes an unauthorized disclosure of classified data has occurred on an information system or network (typically called a "data spill").

(6) This DHA-AI establishes fundamental security education and training standards for original classification authorities, derivative classifiers, declassification authorities, security managers, classification management officers, security specialists, and other personnel whose duties involves the creation, handling, and storage of sensitive or classified information.

d. Refresher/Reoccurring Training

(1) DHA personnel will receive annual refresher training as outlined in Reference (g).

(2) Derivative classifiers (i.e., those who create new documents, including e-mails, based on existing classification guidance), will receive training in derivative classification annually. Derivative classifiers who do not receive training on an annual basis will not be authorized or allowed to access classified information until training is completed.

(3) Declassification authorities must receive annual training, as required by Reference (d) and this DHA-AI.

(4) DHA personnel will receive an Annual Security Refresher, as required.

e. Special Training Requirements

(1) Sensitive and/or CUI/Material requires education and training be provided before, concurrent with, or not later than 30 days following assuming those duties.

(2) Classified Information/Material requires education and training be provided before, concurrent with, or not later than 30 days following assuming those duties.

(3) SCI/Material requires the SSO conduct continuing SCI security education training and awareness to ensure all SCI-indoctrinated individuals are kept apprised of the requirements and guidelines for protecting SCI. Annual training of original classification authorities and annual training for derivative classifiers is required. Refresher training will adhere to the guidelines outlined in Reference (g).

(4) COMSEC

(a) COMSEC training will be completed before assuming duties and will be provided by the Pentagon Force Protection Agency's local COMSEC Office.

(b) Only properly trained security personnel are authorized to operate cryptographic equipment. Further requirements are located in Reference (i).

(5) Management and Oversight Training:

(a) Education and training may be provided before, concurrent with, or not later than 30 days following assuming those duties, unless otherwise specified.

(b) Individuals designated as security managers, classification management officers, security specialists, or any other personnel whose duties significantly involve managing and overseeing classified information must receive training that meets the requirements outlined in Reference (g).

(6) Courier Training is required for all persons performing courier duties. Those individuals must receive training on proper procedures and the proper marking of materials prior to assuming duty per Reference (ab).

3. CLASSIFIED INFORMATION OVERVIEW

a. Types of Classified Information. The three types of classification are identified in Reference (d).

b. Storage, Handling, and Safeguarding

(1) Requirements are listed in References (f), (j), and (n) through (p).

(2) Safeguarding classified information is the responsibility of all who have access to such information. Training in safeguarding procedures must emphasize appropriate policies, procedures, and reporting criteria.

c. Reproduction, Destruction, and Disposal. Requirements are listed in References (f) and (j).

d. Transmission, Transportation, and Shipping

(1) The terms "transmission" and "transportation" of classified material in this DHA-AI refers not only to the physical transfer from a sender to a recipient, but also to the transmission of classified information via connective methods, such as cable or wire, as well as via non-connective methods.

(2) Requirements are listed in Reference (f).

e. Access

(1) Requirements are listed in Reference (f).

(2) SCI-indoctrinated escorts are required when uncleared employees have access to SCI facility areas.

(3) Before being granted access to Confidential, Secret, or TS information, employees will sign a SF 312, "Classified Information Nondisclosure Agreement." Electronic signatures will not be used to execute the SF 312.

f. Emergency Access. Requirements are listed in Reference (f).

4. CLASSIFIED STORAGE FACILITIES

a. Open Storage Facility. An area constructed in accordance with the requirements of this DHA-AI and authorized by the SAO for open storage of classified information.

(1) Requirements are listed in Reference (f).

(2) An employee cleared to at least the Secret level must inspect the open storage area once every 4 hours.

b. Closed Storage Facility. Requirements are listed in Reference (f).

c. Control Measures. DHA will have a system of control measures that ensure access to classified information is limited to authorized persons. Requirements are listed in References (f) and (g).

5. SENSITIVE INFORMATION OVERVIEW

a. Types of Sensitive Information. Requirements are listed in Reference (g).

b. Storage, Handling, and Safeguarding

(1) For storage and handling refer to paragraph 3.a. of this Enclosure.

(2) Safeguarding sensitive information is the responsibility of all who have access to such information.

c. Reproduction, Destruction, and Disposal. Requirements are listed in Reference (f).

d. Transportation

(1) Refer to paragraph 3.d.(1) of this Enclosure.

(2) DD Form 2923 will be used as a cover sheet for covering and transporting all Sensitive material.

6. SCI OVERVIEW

a. Compartments. Compartments include Human Intelligence Control System, Talent Keyhole, Signal Intelligence, and Gamma.

b. Storage, Handling, and Safeguarding

(1) Storage requirements are listed in References (j) through (l).

(2) Handling requirements are listed in References (j) through (l).

(3) Refer to section 3.b.(2) of this Enclosure.

c. Reproduction, Destruction, and Disposal. Requirements are listed in References (e) through (h), and (k).

d. Transmission, Transportation, and Shipping. Requirements are listed in References (f), (g), and (j).

e. Access. Requirements are listed in References (d) and (t).

f. Emergency Access Authority. Requirements are listed in Reference (f).

7. MAILING AND CARRYING CLASSIFIED MATERIALS. Requirements are listed in References (f) and (u).

8. PLANS AND PROGRAMS

a. COMSEC Plan. Requirements are listed in References (f), (h), (i), and (n) through (p).

b. EAP. Requirements are listed in References (f), (i), and (j).

c. Transportation Plan. Requirements are listed in Reference (f).

d. Inspection and Assessment Program. The Inspection and Assessment Program identifies and shares best practices and lessons learned for security implementation to inform decisions about security policy, plans, programs, program management, and resources. Requirements are listed in References (d), (f), (g), and (i).

(1) Inspection Program

(a) Self-inspection requirements are listed in Reference (d).

(b) DoD SCI facility inspections of Mission Services and Counterintelligence and Security Offices are conducted by the Deputy Director, Defense Intelligence Agency. Inspections are conducted on a periodic basis and are based off risk management principles. Further requirements are listed in Reference (i).

(2) Assessment Program

(a) Risk assessment requirements are listed in Reference (f).

(b) Damage assessment requirements are listed in Reference (f).

e. Incident Program

(1) Types of incidents

(a) Security incident types and requirements are listed in Reference (f).

(b) CUI incident requirements are listed in Reference (g), (v), and (w).

(2) Reporting requirements are listed in Reference (d) and (f).

(3) Inquiry and Investigation requirements are listed in Reference (f).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASM	Activity Security Manager
COMSEC	Communications Security
CSSO	Contractor Special Security Official
CSSR	Contractor Special Security Representative
CUI	controlled unclassified information
DAD	Deputy Assistant Director
DHA	Defense Health Agency
DHA-AI	Defense Health Agency-Administrative Instruction
ESTMS	Enterprise Security, Threat Management, and Safety
INFOSEC	Information Security
SAO	Senior Agency Official
SCI	Sensitive Compartmented Information
SIO	Senior Intelligence Official
SOP	Standard Operating Procedure
SSO	Special Security Official
SSR	Special Security Representative
TS	Top Secret
TSCO	Top Secret Control Official

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this DHA-AI.

breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where individuals gain access or potential access to sensitive and classified material, whether physical or electronic for an unauthorized purpose.

CUI. Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. The designation CUI replaces the term "sensitive but unclassified." Additional information is found in Reference (ab).

incident. A security occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

market. A group of Military Medical Treatment Facilities in a geographic area that operates as a system through sharing patients, functions, budget, etc., across facilities in order to improve the delivery and coordination of health services to drive value for beneficiaries.

sensitive position. Any position within or in support of a government agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on national security regardless of whether the occupant has access to classified information and regardless of whether the occupant is an employee, military service member, or contractor. The designation types of Sensitive are Noncritical-sensitive, Critical-sensitive, and Special-sensitive determine the degree to which any person in the position could cause a "material adverse effect on national security."