Defense Health Agency

ADMINISTRATIVE INSTRUCTION

NUMBER 5200.03
July 1, 2021

DAD-A&M

SUBJECT: Operations Security (OPSEC) 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 guidance of References (c) through (i), establishes the Defense Health Agency's (DHA) procedures for the OPSEC Program.

2. APPLICABILITY. This DHA-AI applies to all DHA personnel to include assigned, attached, or detailed Active Duty, Reserve, National Guard members, contractors and subcontractors, when required by the terms of the applicable contract, federal civilians, members of the Commissioned Corps of the Public Health Service, and other personnel assigned temporary or permanent duties at DHA and DHA components (activities under the authority, direction, and control of DHA).

3. POLICY IMPLEMENTATION. It is DHA's policy, pursuant to References (d) through (i) to integrate comprehensive programs, procedures, and processes, throughout DHA locations and levels, to implement compliance with this DHA-AI and the References listed in Enclosure 1.

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 his date in accordance with Reference (c).

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

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

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 Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, as amended
(e) DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019
(f) DoD Instruction 5200.01, Volume 4 "DoD Information Security Program: Controlled Unclassified Information (CUI)", February 24, 2012
(g) DoD 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008, as amended
(h) Office of Management and Budget Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017
(i) DoD 5400.11-R, "DoD Privacy Program," May 14, 2007

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA, in addition to the responsibilities identified in Reference (d) and paragraph 1a in Reference (h) will:

a. Be responsible for overall management, functioning, and effectiveness of the OPSEC Program.

b. Provide adequate funding and resources to effectively implement this Program.

c. Appoint in writing the Senior Agency Official (SAO) and alternate(s).

2. SAO. The DAD-A&M must serve as the SAO and be responsible for directing, administering, and overseeing the OPSEC Program within the Agency, in addition to the responsibilities identified in Reference (g). The SAO must:

a. Appoint in writing the following program officials:

(1) Activity Security Manager (ASM) and alternate(s);

(2) OPSEC Program Manager (PM) and alternate(s); and

(3) OPSEC Program Coordinator (PC) and alternate(s).

b. Assign an Office of Primary Responsibility for the Agency's OPSEC Program.

c. Provide senior level oversight of the OPSEC Inspection and Assessment Program to include self-inspections and random Agency level reviews.

d. Establish and maintain an ongoing Self-inspection and Assessment Program with oversight to evaluate and assess the effectiveness and efficiency of the implementation of the OPSEC Program.

e. Direct, administer, and oversee the disclosure of classified military information to foreign governments, foreign persons, and foreign employees. Coordinate exemptions and waivers with the OPSEC PM.

f. Develop and maintain the Agency's Security Education and Training Program and designate personnel, as necessary, to assist in carrying out this responsibility.

3. ASM. The ASM, is responsible for the management and implementation of the OPSEC Program, in addition to requirements and responsibilities identified in Reference (g).

4. CHIEF, ENTERPRISE SECURITY, THREAT MANAGEMENT, AND SAFETY (ESTMS). The Chief, ESTMS under the authority, direction, and control of the DAD-A&M must:

a. Establish goals, objectives, standards, and conduct education, outreach, and training in support of this DHA-AI.

b. Establish Memorandum of Agreements or Memorandum of Understandings between installation or facility host and tenants.

c. Serve as the Principal Advisor and representative to the ASM in all matters pertaining to this DHA-AI and maintain cognizance of all activity information, personnel, and information systems, physical and industrial security functions to ensure the DHA-AI is coordinated in its execution and inclusive of all requirements.

d. Ensure personnel who perform security duties are kept abreast of changes in policies and procedures, and provided assistance in problem solving.

5. OPSEC PM. The OPSEC PM must:

a. Be responsible for the administration of the OPSEC Program, in addition to responsibilities identified in Reference (h).

b. Assist information owners in promoting information sharing, while safeguarding information that could harm DHA operations or jeopardize information-sharing agreements among stakeholders.

c. Ensure a process is in place to report disclosures of critical information to appropriate channels within DHA so mitigating actions can be implemented. Per References (h) and (i):

(1) Should such disclosure be an actual or possible loss of control, unauthorized disclosure of, or unauthorized access to, personal information, where persons other than authorized users gain access or potential access to such information for other than authorized purposes, the discovering party shall provide notification within 1 hour of such breach to the DHA Privacy Office at (703) 275-6363 and/or dha.privacyofficer@mail.mil.

(2) If such breach is a potential or actual cybersecurity incident, the discovering party shall report this to US-CERT within 1 hour of the cybersecurity incident.

d. Complete the DoD OPSEC Fundamentals Course within 30 days of assignment.

e. Complete the DoD Interagency Operations Security Support Staff (IOSS) Program Manager Course or other DoD Component equivalent course within 90 days of assignment.

6. OPSEC PC. The OPSEC PC must:

a. Provide oversight at their respective DHA facility, and interface with the OPSEC PM as necessary to elevate issues that could affect the DHA as a whole.

b. Complete an approved DoD OPSEC Fundamentals Course within 90 days of assignment.

c. Satisfy both preparatory and sustaining DoD standard education and training requirements within 90 days of assignment.

d. Plan and conduct assessments in collaboration with the information owner responsible for the operation, activity, or exercise. This will be in coordination with the OPSEC PM and supported by ESTMS.

e. Develop and submit facility OSPEC Plan and Annual Program Reviews to the OPSEC PM.

f. Develop and implement standard operating procedures. Submission of standard operating procedures will be to ESTMS for review and approval prior to their execution.

g. Adhere to the requirements listed in Reference (h).

7. CONTRACT OFFICIALS. In conjunction with the Director, DHA, Contract Officials must establish procedures to ensure that contract requirements properly reflect OPSEC responsibilities and that those responsibilities are included in both classified and unclassified contracts per Reference (h).

8. INDIVIDUALS. Individuals identified in the applicability statement must:

a. Adhere to the procedures identified in References (d) through (h).

b. Complete initial OPSEC orientation, provided by the ESTMS team, regarding the DHA OPSEC Program within 30 days of arrival. This initial orientation will provide employees a degree of understanding of OPSEC policies and doctrine that commensurate with his/her responsibilities.

c. Complete mandatory Annual Refresher OPSEC training that reinforces understanding of OPSEC policies and procedures, critical information, and procedures covered in initial and specialized training.

ENCLOSURE 3

PROCEDURES

1. TRAINING. All personnel in DHA, including personnel assigned or detailed Active Duty, Reserve, and National Guard members, federal civilians, members of the Commissioned Corps of the Public Health Service, contractors & subcontractors, and other personnel assigned temporary or permanent duties are required Initial and Annual Refresher OPSEC training.

a. OPSEC Fundamentals Course. All OPSEC PMs and PCs with assigned duties as their primary job shall complete the OPSEC Fundamentals Course within 30 days of assignment.

b. IOSS Program Manager Course. All OPSEC PMs will complete the IOSS PM Course or DoD Component equivalent within 90 days of assignment.

c. OPSEC Awareness Training. All personnel are required to attend initial orientation to the organization's OPSEC Program. Initial orientation is intended to provide employees a degree of understanding of OPSEC policies and doctrine commensurate with their responsibilities.

2. STEPS OF AN OPSEC PROCESS. The OPSEC process is a five element systematic method used to identify, control, and protect critical information and involves Identifying Critical Information, Conducting a Threat Analysis, Conducting a Vulnerability Analysis, Conducting a Risk Analysis, and Applying OPSEC Countermeasures. All elements must be present, per Reference (h).

3. CONTENT REVIEWS. A content review is an evaluation of information intended for release outside the control of the Agency, including release to the public. OPSEC focuses on identifying and protecting the DHA's unclassified information that may individually or in the aggregate lead to the compromise of sensitive and classified information. Additional guidance is found in Reference (h).

4. ASSESSMENTS. Assessments are conducted annually to assess the overall evaluation of the Agency's OPSEC posture to determine the threat to the United States operations and the potential loss of critical information, as further defined in Reference (h).

5. SURVEYS. Surveys are conducted every 3 years, or when required, and involve analyzing activities associated with specific operations or programs to determine if there is adequate protection of critical information from adversary intelligence exploitation and propose countermeasures, as discussed in Reference (h).

6. INTERNET SERVICES. When an individual is requested to furnish personal identifiable information via a DoD Internet Service and the information is not maintained in a Privacy Act system of record, the solicitation of such information requires a privacy advisory be provided. The privacy advisory informs the individual as to why the information is being solicited and how the information will be used. Additional guidance is in Reference (f).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

A&M	Administration and Management
ASM	Activity Security Manager
DAD	Deputy Assistant Director
DHA	Defense Health Agency
DHA-AI	Defense Health Agency-Administrative Instruction
ESTMS	Enterprise Security, Threat Management, and Safety
IOSS	Interagency Operations Security Support Staff
OPSEC	Operations Security
PC	Program Coordinator
PM	Program Manager
SAO	Senior Agency Official

PART II. DEFINITIONS

These terms and their definitions are for the purposes of this DHA-AI.

critical information. Information about DoD activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary, may prevent or degrade mission accomplishment, cause loss of life, or damage friendly resources.

OPSEC. A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.

public. Anyone outside of the intended audience. An intended audience are individuals and/or groups identified by the originator/owner with authority to grant access to sensitive and/or classified information and material.