Defense Health Agency

ADMINISTRATIVE INSTRUCTION

NUMBER 003
July 23, 2018

J-1, MAB

SUBJECT: Physical Security Program

References: See Enclosure 1.

1. PURPOSE. This Defense Health Agency-Administrative Instruction (DHA-AI), based on the authority of References (a) through (c), and in accordance with the guidance of References (d) through (l), (n), and (o):

a. Establishes the Defense Health Agency's (DHA) procedures for the implementation of an agency-wide Physical Security Program. The DHA Physical Security Program is concerned with active and passive measures designed to prevent unauthorized physical access to DHA personnel, equipment, leased space, information; and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.

b. Incorporates, updates, and cancels Reference (m).

2. APPLICABILITY. This DHA-AI applies to:

a. All DHA personnel to include: assigned, attached, or detailed 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) and the National Capital Region Medical Directorate activities (centers, clinics, and Medical Treatment Facilities (MTFs)).

b. All visitors while within DHA-leased space.

c. Any members of organizations co-located within government-leased spaces in which DHA is the largest organization.

3. POLICY IMPLEMENTATION. It is DHA's policy, pursuant to References (d) through (g), that all DHA sites execute a DHA Physical Security Program based on the requirements set forth in this DHA-AI. Each respective DHA site will execute the requirements of this DHA-AI as it pertains to specific physical security processes and procedures. How particular DHA sites execute the requirements in this DHA-AI will be outlined in site-specific Standard Operating Procedures (SOPs), and/or a separate site-specific physical security plan. All such correspondence(s) will be submitted to DHA's J-1, Mission Assurance Branch (MAB), Physical Security, for review and approval prior to implementation. Any requested exemptions to this DHA-AI will be submitted to the Chief, MAB, who, in consultation with the DHA Front Office and the Office of the General Counsel, will approve or deny the exemption.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Not cleared for public release**. This DHA-AI is available to users with Common Access Card (CAC) authorization on 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 DHA-Procedural Instruction 5025.01 (Reference (c)).

R. C. BONO
VADM, MC, USN
Director

Enclosures
1. References
2. Responsibilities
3. Procedures
4. Medical Treatment Facility Security Level Determination

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 21, 2015
(d) DoD 5200.08-R, "Physical Security Program," April 9, 2007, as amended
(e) DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended
(f) Directive-Type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access Control," November 20, 2015, as amended
(g) DoD Directive 5105.21, Volume 2, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security," October 19, 2012
(h) DHA-Administrative Instruction 078, "Antiterrorism (AT) Program," December 22, 2014, as amended
(i) Code of Federal Regulations, Title 41, Parts 102-71
(j) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
(k) United States Code, Title 18, Section 930
(l) DHA Memorandum, "Possession of Privately Owned Firearms by Department of Defense Personnel Not Related to the Performance of Official Duties," June 27, 2017
(m) TRICARE Management Activity (TMA) Standard Operating Procedures Number 003, "TRICARE Management Activity Security Program," May 23, 2006 (hereby cancelled)
(n) DHA-Administrative Instruction 066, "Director's Critical Information Requirements (DCIRs) Situation Report (SITREP)," July 21, 2017
(o) The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, 2nd Edition, November 2016

ENCLOSURE 2

RESPONSIBILITIES

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

a. Establish and implement the DHA Physical Security Program in accordance with Reference (d).

b. Designate the Chief, MAB, as the DHA Physical Security Program Manager (PM) to oversee the DHA Physical Security Program.

c. Appoint in writing, a Designated Official (DO), Senior Official (SO), or Senior Agency Official (SAO) for each DHA facility or geographic location.

d. Allocate resources to the DHA Physical Security Program, as applicable.

2. CHIEF, MAB. The Chief, MAB, will:

a. Serve as the DHA's Physical Security PM and provide oversight for the DHA Physical Security Program.

b. Direct the coordination of the DHA Physical Security Program with other security disciplines organic to, or supporting the DHA, such as personnel security, operations security, information security, counterintelligence, antiterrorism, law enforcement, and the insider threat program, in order to provide an integrated and coherent overall security effort.

c. Ensure physical security incidents are reported, tracked in accordance with References (h) and (n) and, when necessary, inquiries or investigations are conducted.

d. Establish and coordinate requirements for the acquisition of any physical security system and/or equipment agency-wide.

e. Advise the DO/SO/SAO of their responsibilities as it relates to the DHA Physical Security Program within their Area of Responsibility (AOR).

f. Identify applicable certifications, training, qualifications, and suitability requirements for DHA dedicated security forces to include military, civilian, and contract support personnel, in security positions in terms of security functional tasks.

g. Review and approve all Facility Security Assessment results involving DHA-leased space, to include the proposed Facility Security Level (FSL).

h. Ensure physical security requirements within the DHA classified collateral areas and sensitive compartmented information facilities comply with Reference (g).

i. Review site-specific SOPs developed as supplements to this DHA-AI, and coordinate with the DO/SO/SAO on approval of such documents.

j. Ensure agency-wide compliance and uniform execution of the DHA Physical Security Program.

k. Ensure all sites are assessed in accordance with Enclosure 3 of this DHA-AI.

l. Provide oversight and management of all security containers, across DHA, through its lifecycle of inventory, maintenance, repair, and disposal.

3. DO/SO/SAO. The DO/SO/SAO will:

a. Assume responsibility for the execution of the DHA Physical Security Program within their AOR.

b. Appoint, in writing, a Physical Security Representative (PSR) to assist in the execution of the following functions; however, the responsibility remains with the respective DO/SO/SAO. The DO/SO/SAO, assisted as appropriate by a PSR, will:

c. Coordinate site assessments in accordance with Enclosure 3 of this DHA-AI.

d. Develop site-specific SOPs, in coordination with the Physical Security PM, to meet any specific needs of their AOR not addressed in this DHA-AI.

e. Ensure personnel are aware of their responsibilities in support of the Physical Security Program.

f. Participate in Facility Security Assessments to include proposed FSL determinations.

g. Conduct physical security inquiries and investigations as directed by the Physical Security PM or designee.

h. Liaise with local antiterrorism, counterintelligence, and law enforcement entities to ensure mutual awareness and support of local response programs and suspicious activity reporting procedures at the direction of the Physical Security PM.

i. Consolidate and submit site-specific funding and acquisition requests regarding physical security equipment and services to the Physical Security PM.

j. Report all physical security incidents to the Physical Security PM; incidents requiring notification of the DHA Duty Officer are reported in accordance with Reference (n).

k. Develop site-specific SOPs to meet any specific needs within the AOR not addressed in this DHA-AI.

l. Manage all keys and access media pertaining to the DHA leased-spaces within AOR.

ENCLOSURE 3

PROCEDURES

1. SOPs. Site-specific SOPs will outline physical security measures, processes, and procedures unique to a specific DHA site. It may also address elements not included in this DHA-AI, but subjecting the execution of the DHA Physical Security Program at a particular site. DHA Physical Security Program SOPs will be reviewed annually, at a minimum, as often as there is a substantial change, or when directed by the Physical Security PM. All DHA Physical Security Program SOPs must be coordinated through the Physical Security PM.

2. PHYSICAL SECURITY ASSESSMENTS. Physical security assessments will be conducted at all DHA locations in accordance with the following criteria:

a. A physical security self-assessment will be conducted annually by the site DO/SO/SAO as applicable, or an appointed member of their staff.

b. A higher headquarters physical security assessment will be conducted triennially by the Physical Security PM, or a member of his/her staff.

c. When possible, physical security assessments will be conducted in conjunction with required vulnerability assessments (Reference (h)).

d. Physical security assessments will be conducted using benchmarks promulgated by the Physical Security PM, based on applicable DoD-approved benchmarks, Interagency Security Committee, and Unified Facilities Criteria standards, as well as guidance from the combatant command or host installation in which the DHA site operates. The MTFs, in consultation with the MTF's Director/Commander, will be assessed using the DHA-approved benchmarks (Enclosure 4), in addition to the aforementioned benchmarks and standards.

3. CONTROLLED AND RESTRICTED AREAS. Areas within DHA space designated as "Restricted" or "Controlled" must be approved by the Physical Security PM (Reference (d)).

4. SECURITY INCIDENTS. DHA personnel are responsible for reporting any physical security incidents immediately to their respective DO/SO/SAO, as well the Physical Security PM. Failure to report security incidents may result in administrative or disciplinary action. Security incidents are defined in accordance with Reference (k), and may include, but are not limited to:

a. Theft within DHA space;

b. Unauthorized access to DHA space;

c. Failure to properly display valid identification (ID) while in DHA space;

d. Destruction of DHA property; and

e. Any event adversely affecting the physical security posture of a DHA location.

5. KEY AND ACCESS MEDIA MANAGEMENT. A complete inventory of keys and other access media, to include blanks, will be completed annually. Specific key control procedures may be outlined in a local physical security SOP as approved/coordinated by the Physical Security PM.

6. ACCESS CONTROL. Standards for access to DHA space will meet the requirements put forth in References (d) through (g) and executed according to the following:

a. The CAC is the principal identity credential to facilitate access into DHA space. The CAC, upon presentation at a DHA access control point, is accepted as valid authorization for entry; however, additional screening may be required based on the site's FSL or host facility security posture;

b. Areas within DHA space, in which activities deemed sensitive by leadership are conducted, may require additional access control measures, beyond the normal; and

c. DHA sites not able to meet these requirements must submit an interim plan for mitigating current deficiencies and recommendations for future compliance to the Physical Security PM.

7. VISITORS. All DHA sites will have a green or red visitor badge system established by the assigned PSR and approved by the Physical Security PM. Persons visiting DHA space will be considered for escorted (with a red badge), or unescorted (with a green badge) visitation based on the following criteria:

a. Unescorted visitors to DHA space will be given a green badge and must possess one of the following forms of ID:

(1) DoD CAC; and

(2) U.S. Government-issued, authenticated Federal Personal ID Verification credentials;

b. Other personnel needing regular access to DHA space, due to the nature of their work, will not be issued a CAC or Federal Personal ID Verification. They may be authorized a local alternative badge as outlined in the local site-specific physical security SOPs. Alternative badges must have an expiration date and time group assigned to the credential, and the holder of the credential must provide proofed and vetted ID in accordance with Reference (f) and as outlined in the local site-specific physical security SOPs;

c. Visitors not possessing one of the forms of ID specified in paragraph 7.a. will require an escort. Escorted visitors will be given a red badge and must be sponsored by a DHA employee who currently works within the space;

d. A visitor may not escort another visitor; and

e. A visitor badge will not be considered valid ID for access into DHA space.

8. ID BADGES

a. ID badges, as listed in subparagraph 7.a., will be displayed above the waist and fully visible at all times while in DHA space.

b. Lost, missing, or stolen badges will be reported immediately to the site PSR.

c. ID badges will not be shared or loaned. The use of another individual's badge for access is considered a security incident and must be immediately reported to the site PSR.

9. PROHIBITED WEAPONS. In accordance with Reference (k), the following are considered weapons and are thereby prohibited within any DHA-leased space:

a. Any loaded or unloaded pistol, rifle, shotgun, or other device which is designed, or may be readily converted, to expel a projectile by the ignition of a propellant, compressed gas, or spring;

b. Any bow and arrow, crossbow, blowgun, spear gun, hand-thrown spear, slingshot, irritant gas device, explosive device, or any other device designed to discharge missiles;

c. Any other weapon, device, instrument, material, or substance, animate or inanimate, that is used for or is readily capable of causing death or serious bodily injury. These include, but are not limited to, metal knuckles, batons, blackjacks, stun devices, and any weaponry with a blade exceeding 2.5 inches in length;

d. Any weapon the possession of which is prohibited under the laws of the state in which the DHA site operates;

e. Multiple containers of, or a single device containing more than one ounce (28 grams) of oleoresin capsicum (OC), also known as "OC spray" or "pepper spray";

f. Any OC spray or pepper spray container not designed and commercially sold specifically for personal protection and labeled by the manufacturer with the exact type and amount of chemical agent; and

g. The above prohibited weapons are subject to immediate confiscation by Federal or local law enforcement personnel supporting DHA sites. Confiscation of the prohibited weapons may be deemed permanent, and the confiscated property will be considered non-redeemable.

h. In accordance with Reference (l), waivers to this DHA-AI may be addressed to the Physical Security PM.

ENCLOSURE 4

MEDICAL TREATMENT FACILITY SECURITY LEVEL DETERMINATION

1. FSL. The FSL determination serves as the basis for implementing protective measures at Federal facilities and devising an appropriate risk management strategy to mitigate risks. It is based on the unique characteristics and the Federal occupant(s) of each facility. The five factors quantified to determine the FSL are mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. The FSL determination ranges from a Level I (lowest risk) to Level V (highest risk). Once the FSL is determined, physical and operational countermeasures and the appropriate level of protection may be implemented to minimize risk to the facility and its occupants.

2. FSL MATRIX. The FSL determination is derived using the FSL matrix, which is comprised of five equally weighted security evaluation factors with corresponding points of 1, 2, 3, or 4 for each factor (Reference (o)). Given the unique and critical mission of MTFs, the factors and standards used to determine a Federal FSL have been modified to better address MTF-specific conditions. The five factors quantified to determine an MTF FSL are mission criticality, facility size, threat to hospital, emergency room (ER), and behavioral health. The FSL determination matrix for MTFs is listed below in Table 1.

Table. The Facility Security Level Determination Matrix

Factor	Points				Score
	1	2	3	4	
Mission Criticality	LOW	MEDIUM	HIGH	VERY HIGH	
Facility Size (Sq. Ft.)	≤ 49,999	50,000-499,999	500,000-999,999	≥ 1M	
Threat to Hospital	LOW	MEDIUM	HIGH	VERY HIGH	
Emergency Room	LOW	MEDIUM	HIGH	VERY HIGH	
Behavioral Health	LOW	MEDIUM	HIGH	VERY HIGH	
				SUM	
Facility Security Level	0-7 Points LOW	8-12 Points MEDIUM	13-17 Points HIGH	18-20 Points VERY HIGH	**Total**

3. FSL SCORING CRITERIA

a. Mission Criticality (Access to Care)

Value	Points	Criteria	Examples
Very High	4	Time to nearest urgent medical support ≥ 60 minutes	
High	3	Time to nearest urgent medical support 40–60 minutes	
Medium	2	Time to nearest urgent medical support 20–40 minutes	
Low	1	Time to nearest urgent medical support ≤ 20 minutes	
Intangible Adjustment			If needed

b. Threat to Hospital

Value	Points	Criteria	Examples
Very High	4	Determined by local threat assessment	
High	3	Determined by local threat assessment	
Medium	2	Determined by local threat assessment	
Low	1	Determined by local threat assessment	
Intangible Adjustment			If needed

c. Emergency Room

Value	Points	Criteria	Examples
Very High	4	State designated/sponsored Level I trauma center	Tripler, Brooke Army Medical Center, Madigan, Port Smith
High	3	Level I capable trauma center	Does MTF meet Level 1 trauma criteria, but not sanctioned by the state of operation (state reimbursement for civilian care).
Medium	2	Level II capable trauma center	Must have 24-hour ER, Operating Room, Intensive Care Unit, and General Surgery

Low	1	Level III capable trauma center	Surgical procedures within 30 minutes and 24-hour ER
Intangible Adjustment			If needed

d. Behavioral Health

Value	Points	Criteria	Examples
Very High	4	Inpatient care Average behavioral health outpatient ≥ 500 total daily appointments	Secured ward Residential substance abuse program
High	3	Average behavioral health outpatient 250–499 total daily appointments	
Medium	2	Average behavioral health outpatient 50–249 total daily appointments	
Low	1	Average behavioral health outpatient ≤ 49 total daily appointments	
Intangible Adjustment			If needed

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AOR	Area of Responsibility
CAC	Common Access Card
DHA	Defense Health Agency
DHA-AI	Defense Health Agency-Administrative Instruction
DO	Designated Official
ER	emergency room
FSL	Facility Security Level
ID	identification
MAB	Mission Assurance Branch
MTF	Medical Treatment Facility
OC	oleoresin capsicum
PM	Program Manager
PSR	Physical Security Representative
SAO	Senior Agency Official
SO	Senior Official
SOP	Standard Operating Procedure

PART II. DEFINITIONS

DO. The highest ranking official of the primary occupant agency of a Federal facility, or, alternatively, a designee selected by mutual agreement of occupant agency officials.

FSL. A categorization based on the analysis of several security-related facility factors, which serves as the basis for the implementation of physical security measures specified in Interagency Security Committee standards.

passive measures. Defensive countermeasures established to protect personnel, facilities, and intellectual property against anticipated threats. These may include the effective use of

architecture, landscaping, and lighting to aid in deterring, disrupting, or mitigating potential threats.

Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

restricted area. An area (land, sea, or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized by the installation/activity and the commander/director, properly posted, and will employ physical security measures. Additionally, controlled areas may be established adjacent to restricted areas for verification and authentication of personnel.

security container. As identified in this DHA-AI, security containers are considered vault doors with a General Services Administration-approved combination lock or padlock, safes, or cabinets. Security containers protecting or securing classified areas or material is the responsibility of the Special Security Office.

vulnerability assessment. The comprehensive evaluation of an installation, facility, or activity to determine preparedness to deter, withstand, and/or recover from the full range of adversarial capabilities based on the threat assessment, compliance with protection standards, and risk management.