Defense Health Agency

ADMINISTRATIVE INSTRUCTION

NUMBER 5210.01
July 12, 2023

Director, J-3

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) and (b), and in accordance with the guidance of References (c) through (ar), 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, facilities, infrastructure, resources, and critical information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the DHA. Additional guidance is available from DHA J-3 Protection Operations (J-34). The J-34 central phone number is (703) 681-2206 and the SharePoint URL is https://info.health.mil/sites/dos/J3/J34-Home. The Physical Security Section email box is dha.physec@health.mil.

2. APPLICABILITY. This DHA-AI applies to:

a. DHA and DHA Components (activities under the authority, direction, and control of DHA).

b. DHA personnel to include: assigned or attached active duty and Reserve Component Members, federal civilians, contractors (when required by the terms of the applicable contract), and other personnel assigned temporary or permanent duties at DHA and DHA Components.

c. Visitors while within DHA-leased space.

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

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

(h), that all DHA sites:

a. Execute a DHA Physical Security Program based on the requirements set forth in this DHA-AI.

b. Outline local processes and procedures by which a particular site executes these requirements in site-specific standard operating procedures (SOP), local policy letters, or a separate site Physical Security plan.

c. Submit such correspondence to the DHA Physical Security Section for review and approval prior to implementation.

4. CANCELED DOCUMENTS. This DHA-AI cancels the following: DHA-AI 003, "Physical Security Program," July 23, 2018.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. PROPONENT AND WAIVERS. The proponent of this publication is the Director of Operations (J-3). When Activities are unable to comply with this publication the activity may request a waiver. See Enclosure 3 for specific waiver process guidance.

8. RELEASABILITY. **Cleared for public release**. This DHA-AI is available on the Internet from the Health.mil site at: https://health.mil/Reference-Center/Policies and is also available to authorized users from the DHA SharePoint site at: https://info.health.mil/cos/admin/pubs/SitePages/Home.aspx.

9. 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).

10. FORMS. The following forms can be found at: https://info.health.mil/cos/admin/DHA_Forms_Management/Lists/DHA%20Forms%20Management/AllItems.aspx

a. DHA Form 238, Request for Waiver from Security Criteria

b. DHA Form 239, Physical Security Project Request

c. DHA Form 260, Notice of Security Incident

CROSLAND.TELITA.1017383040 Digitally signed by CROSLAND.TELITA.1017383040 Date: 2023.07.12 10:52:38 -04'00'

TELITA CROSLAND
LTG, MC, USA
Director

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

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.0, "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, as amended
(c) DHA-Procedural Instruction 5025.01, "Publication System," April 1, 2022
(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) DoD Manual 5200.08, Volume 3, "Physical Security Program: Access to DoD Installations," January 2, 2019, as amended
(g) 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
(h) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended
(i) DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 1, 2012, as amended
(j) DHA-Administrative Instruction 078, "Antiterrorism (AT) Program," September 1, 2022, as amended
(k) United States Northern Command Instruction 10-222, "USNORTHCOM Force Protection Mission and Antiterrorism Program," November 10, 2021[1]
(l) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
(m) CJCSM 3150.05D, "Joint Reporting System Situation Monitoring Manual," January 31, 2011, as amended
(n) DHA-Procedural Instruction 3700.01, "Director's Critical Information Requirements (DCIR) Situation Reports (SITREP)," October 4, 2019, as amended
(o) Homeland Security Presidential Directive-12, Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
(p) Federal Information Processing Standard 201-3, "Personal Identity Verification (PIV) of Federal Employees and Contractors," January 2022
(q) Items Prohibited from Federal Facilities: An Interagency Security Committee Standard, February 2013
(r) Code of Federal Regulations, Title 18
(s) Code of Federal Regulations, Title 41
(t) Joint Publication 3-26, "Joint Combating Terrorism," July 30, 2020[2]
(u) Unified Facilities Criteria 4-020-01, "DoD Security Engineering Facilities Planning Manual," September 11, 2008

[1] This reference is available at: https://portal.noradnorthcom.mil/library/pubs/sitepages/home.aspx
[2] This reference is available at: https://jdeis.js.mil/jdeis/index.jsp?pindex=27&pubId=705

(v) Unified Facilities Criteria 4-022-02, "Selection and Application of Vehicle Barriers," June 8, 2009, as amended
(w) Intelligence Community Standard 705-1, "Physical and Technical Security Standards For Sensitive Compartmented Information Facilities," September 17, 2010
(x) Intelligence Community Directive 705, "Sensitive Compartmented Information Facilities," May 26, 2010
(y) Intelligence Community Tech Specs for Intelligence Community Directive/Intelligence Community Standard 705, "Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.5," March 13, 2020, as amended
(z) DoD Manual 5100.76, "Physical Security of Sensitive Conventional Arms, Ammunition and Explosives," April 17, 2012, as amended
(aa) Defense Explosive Safety Regulation 6055.09, Edition 1, January 13, 2019
(ab) Unified Facilities Criteria 4-510-01, "Design: Medical Military Facilities," May 30, 2019, as amended
(ac) Code of Federal Regulations, Title 21
(ad) Code of Federal Regulations, Title 7
(ae) Code of Federal Regulations, Title 9
(af) Code of Federal Regulations, Title 42
(ag) DoD Instruction 5210.88, "Security Standards for Safeguarding Biological Select Agents and Toxins," May 26, 2020
(ah) DoD Instruction 5200.48, "Controlled Unclassified Information," March 6, 2020
(ai) DoD Instruction 3020.45, "Mission Assurance Construct," August 14, 2018
(aj) National Institute of Justice Standard 0101.06, "Ballistic Resistance of Body Armor," July 2008
(ak) DHA-PM 4500.01, Fleet Management, July 9, 2021
(al) Unified Facilities Criteria 4-141-04, "Emergency Operations Center Planning and Design," July 15, 2008, as amended
(am) Homeland Security Presidential Directive-5, "Management of Domestic Incidents," February 28, 2003
(an) DoD Instruction O-2000.16, Volume 2, "DoD Antiterrorism (AT) Program Implementation: DoD Force Protection Condition (FPCON) System, "November 17, 2016, as amended
(ao) DoD Instruction 3025.21, "Defense Support of Civilian Law Enforcement Agencies," February 27, 2013, as amended
(ap) DoD Manual 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 25, 2017
(aq) DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," April 5, 2019
(ar) The Risk Management Process: An Interagency Security Committee Standard, 2nd Edition, August 2013, as amended[3]

[3] This reference can be found at: https://www.cisa.gov/sites/default/files/publications/The%20Risk%20Management%20Process%20-%202021%20Edition.pdf

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA:

a. Will maintain responsibility for the DHA Physical Security Program.

b. Designates the DHA Chief, Protection Operations (J-34) as responsible for managing and executing the DHA Physical Security Program enterprise-wide (E-W).

c. Will allocate funding and other resources, based on availability, to the DHA Physical Security Program, as appropriate.

2. DIRECTOR OF OPERATIONS J-3. The Director, J-3 will:

a. Provide executive-level oversight, direction, and support to the DHA Chief of Protection Operations in the execution of the tasks and responsibilities indicated below.

b. Advocate for funding and appropriate resources to execute the DHA Physical Security Program.

3. DHA CHIEF, PROTECTION OPERATIONS. The DHA Protection Operations Division East Hub supports Markets in the eastern United States and Defense Health Agency Region-Europe (DHAR-E). The West Hub supports Markets in the western United States and Defense Health Agency Region Indo-Pacific (DHAR-IP).

a. The DHA Chief, Protection Operations, as the Office of Primary Responsibility, is tasked with the E-W uniform implementation and execution of the DHA Physical Security Program and its support to the overall mission assurance strategy.

b. In the execution of this role, the DHA Chief, Protection Operations will:

(1) Direct the coordination of the DHA Physical Security Program with other security disciplines organic to, or in support of the DHA, such as personnel security, operations security, information security, counterintelligence, Antiterrorism (AT), and the insider threat program, in order to provide an integrated and coherent overall security effort.

(2) Execute the strategic physical security planning function.

(3) Develop and maintain a single source document that states the common DHA security mission and vision, and, through a strategy to task process, provides guidance concerning all physical security-related activities.

(4) Provide a broad perspective on physical security policy reviews. Reviews policy documentation and recommends changes to support developing security concepts and doctrine.

(5) Provide DHA advocacy for acquisition, sustainment, and research and development in support of all physical security systems acquired to meet DoD policy requirements. Validate the requirement of any physical security system or equipment E-W.

(6) Represent DHA at the Security Enterprise Executive Board in support of the DoD Mission Assurance Strategy and Reference (i).

(7) Provide physical security strategic direction, policy, planning guidance, program management, and deficiency and waiver control.

(8) Provide strategic direction, policy, and planning guidance for E-W security and contingency planning, in accordance with governing DoD issuances and DHA publications.

(9) Perform DHA E-W security Planning, Programming, Budgeting, and Execution (PPBE) and consider the impact of risk for DHA sites, facilities, as well as other locations where the DHA is the lead organization with physical security responsibility.

(10) Advocates for security funding to support Direct Reporting Organizations (DRO), field activities, and Combat Support requirements.

(11) Manage the DHA Risk-Management program. The Physical Security Program Manager (PM) is the Senior Security Advisor to the DHA Chief, Protection Operations and leads this capability.

(12) Perform Capacity Building Operations. Capacity Building, also known as Building Partnership Capacity (BPC), will require close communication with the DRO and field activities staff. Responsibilities pursuant to Capacity Building include, but are not limited to:

(a) Identify mission partner capability gaps in supporting DRO and field activities and contingency plans.

(b) Develop courses of action (COA) to mitigate capability gaps.

(c) Liaise with the Military Departments, DoD Components, and federal partners and to provide them with training and mentorship in order to develop security capacity.

(d) Provide training venues and opportunities to partner with security personnel in the DHA enterprise.

(13) Establish a DHA Security Assessment Team (described in Enclosure 3 of this DHA-AI), in order to facilitate headquarters (HQ) level AT Program reviews, assessments, and inspections. Develop E-W triennial assessment and inspection schedule.

(14) Develop and issue standards for training, qualification, and suitability requirements for dedicated security guards, as well as arming requirements to include firearms and non-lethal weapons (NLW) qualification and training.

(15) Approve security guard capabilities and mission essential task lists, establish requirements and program for standing contingency capability, and plan/program contingency backfill capability, if needed.

(16) Conduct physical security strategic analysis involving the conduct of mission and vision analysis in order to determine roles, duties, and responsibilities of security guards.

(17) Provide security guard manpower and equipment oversight and coordination.

4. DHA PHYSICAL SECURITY PROGRAM MANAGER (PM). The DHA Physical Security PM will ensure E-W compliance and uniform execution of the Physical Security Program to include:

a. Consolidate E-W PPBE funding and acquisition requests regarding physical security equipment and services for submission to the DHA Chief of Protection Operations.

b. Develop standards and procedures for conducting physical security inquiries, investigations, and assessments as required and providing reports to the DHA Chief of Protection Operations.

c. Provide support for the DHA Chief of Protection Operations mission to strategically source DHA Physical Security requirements.

d. Provide guidance to DHA Security Assessment Team in accordance with DoD and DHA requirements, concerning AT Program reviews, assessments, and inspections.

e. Manage DHA Security Waiver Control program. Review and provide feedback on waiver requests, in close coordination with DRO and field activity staffs.

f. Manage Integrated/Electronic Security Systems (ESS) programs. Work with DRO, field activities, and DoD Life Cycle Management Center, Force Protection Division to develop and execute projects. Collaborate with physical security experts at subordinate organizations to program for DRO, field activities, and Combat Support needs and sustainment.

g. Responsible for development and update to all Physical Security Program related documents and publications.

h. Provide subject matter expertise for the areas of physical security, use of security guards, resource protection, NLW employment and incident reports. Recommend program changes to DHA Chief of Protection Operations supporting the development of future physical security

concepts and guidance.

i. Provide training tools and products, including but not limited to Mission Assurance Risk Management System (MARMS), Enterprise Protection Risk Management (EPRM) for the DHA community, in the most cost-effective delivery mediums available.

j. Develop and distribute standardized security-related training lesson plans.

k. Provide guidance and training expertise as part of the lessons learned process.

l. Manage current and future requirements based on operational deficiencies and provide requirement oversight in the development and review of emerging technology to fulfill operational capabilities.

m. Facilitate development of physical security concepts by drafting, reviewing, and recommending changes to guidance, and providing subject matter expertise to participate in conferences and committees in order to execute all aspects of the security mission.

n. Contribute to a single source document that states the common Protection Operations mission and vision and through a strategy to task process, serving as the source document for all DHA security activities to include physical security.

o. Manage DHA security guard weapons and equipment program.

p. Coordinate E-W security guard vehicle configuration and mission support needs with the Vehicle and Equipment Management Support Office as needed. Support security guard vehicle inquiries and consult with Vehicle and Equipment Management Support Office as needed for resolution.

q. Provide critical analysis when developing future concepts of security guard employment.

r. Develop security guard mission essential task lists.

5. DHA SPECIAL SECURITY OFFICER. The Special Security Officer is responsible for establishing and approving all physical security requirements within DHA Classified Collateral Areas and Sensitive Compartmented Information Facilities (SCIF) as per References (g) and (h). The Special Security Officer will:

a. Provide guidance and support to DRO and field activities and DHA facilities concerning physical security requirements for Classified Collateral Areas, SCIFs, and all other areas involving classified information or material.

b. Coordinate and work with the host or parent installation's physical and information security offices and law enforcement services as needed.

6. DRO AND FIELD ACTIVITIES DIRECTORS. The DRO, Field Activities Director, Designated Official (DO), or Senior Official (SO), are responsible for the execution of the DHA Physical Security Program and their assigned facilities in accordance with References (d) through (af). The DRO and field activities Director, DO, or SO or a member of their staff, whom they designate in writing, will:

a. Coordinate with their assigned Physical Security Officer or designated security representative, to include DRO and field activities office, if necessary, to clarify any issues concerning the execution of the Physical Security Program in their assigned facilities.

b. Develop site-specific Facility or Physical Security Plan or SOP. NOTE: DHA Tenants of host DoD installations will partner and liaise with the responsible installation security/law enforcement/AT office to meet any local or specific standards not addressed in this DHA-AI.

c. Ensure that personnel in their assigned facilities are aware of their responsibilities in support of the DHA Physical Security Program.

d. Maintain liaison with host or parent DoD installations, base clusters and supporting host-nation security agencies, and civil authorities, as required. Responsibilities for liaison may be retained by higher authority or delegated as local circumstances dictate.

e. Identify and consolidate site-specific funding and acquisition requests regarding physical security equipment and services for submission to DRO and field activities Director.

f. Report all physical security incidents in accordance with Enclosure 3. Installation and law enforcement incident reports could be required by other organizations.

g. Manage credentials, keys, and media pertaining to access to DHA facilities or controlled space. NOTE: DHA security personnel manage and control access to DHA facilities, resources, controlled areas, restricted areas in accordance with this DHA-AI.

h. Ensure assessments are conducted in accordance with DoD program requirements, as well as Enclosure 3 of this DHA-AI. Participate in Facility Security Assessments (FSA) to include proposed Facility Security Level (FSL).

i. Ensure the development of and approve site Facility or Physical Security Plans and Occupant Emergency Plans. Direct changes, updates, or rewrites as needed based on changes to mission, security environment, or other factors.

j. Execute DHA Risk-Management program for their assigned facilities and coordinate closely with DRO and field activities Directors and host installations, if needed, in order to:

(1) Identify, plan, and program for security requirements directly impacting risk management.

(2) Document and submit security waiver requests to the DRO and field activities Director for coordination and review, prior to submitting to DHA Chief of Protection Operations.

(3) Ensure assigned Defense Critical Assets (DCA), Task Critical Assets (TCA), Tiered Assets, and other protection level (PL) resources, security deficiencies, vulnerabilities, compensatory measures, planned projects, etc., are documented via MARMS.

k. Ensure FSAs are conducted for off-installation, General Services Administration (GSA)-leased facilities or space to coordinate with the DRO and field activities Director concerning recommendations prior to FSL determinations.

l. Stand-alone, geographically separated facilities (GSF), dispersed sites, and other like facilities not located on a DoD installation locally implement Physical Security Programs that cover resource protection, physical security, and access control. Those DHA sites and facilities that fall under a parent DoD installation provide required information to their parent installation for inclusion in the installation AT plan, defense plan, or similar document. Parent installations typically consolidate tenant organization inputs and provide administrative support and guidance for conducting the EPRM. The DRO and field activities Director, DO, or SO present the EPRM results and potential COAs to the responsible installation commander's Integrated Defense Council or other responsible council or committee in order to make risk management decisions. Document approved COAs in the host or parent installation's AT, and installation security plan (ISP) or installation defense plan (IDP). The DRO and field activities Director, DO, or SO ensures appropriate support agreements are in place and sufficiently address security and law enforcement needs at the location.

(1) GSFs actively participate in the host or parent installation's EPRM process to ensure the criticality of DHA assets is adequately considered. As directed by the Installation Commander, GCC and consistent with DHA directives and local memorandums of understanding, support may include security guard participation to secure mission assets in their immediate work areas, sites, facilities, compounds, etc.

(2) GSFs ensure asset criticality is considered during the development and review of a support agreement. The parent or host installation executes COAs to create desired AT and security effects in order to mitigate risk to the assets in accordance with the Installation Commander or GCC's and DRO and field activities Director, DO, or SO risk tolerance decision.

(3) DRO and field activities with existing support agreements ensure DHA personnel, assets, and associated COAs are included within the parent or host installation's EPRM process, contained in the IDPs or ISPs, and reviewed annually.

m. Ensure assigned DCA, TCA, Tiered Assets and other PL resources, security deficiencies, vulnerabilities, compensatory measures, planned projects, etc., are documented via MARMS.

ENCLOSURE 3

PROCEDURES

1. SOP. A site-specific SOP or Physical Security Plan will outline physical security measures, processes, and procedures unique to a specific DHA facility. It may also address elements that impact the execution of the DHA Physical Security Program at a particular site (e.g., medical center, hospital, or clinic) but are not included in this DHA-AI. DHA Physical Security Program SOPs or Physical Security Plans will be reviewed annually, when there is a substantial change (e.g., large gain or loss of occupants, new or renovated facilities, significant change of baseline threat, that makes portions of the plan or SOP ineffective or hazardous to execute), or when directed by the DHA Protection Operations. DHA physical security SOPs or Physical Security Plans must be approved by the individual responsible for the execution of the Physical Security Program in their assigned facilities.

2. PHYSICAL SECURITY ASSESSMENTS. Conduct physical security self assessments annually at all DHA sites and facilities, consisting of the following:

a. An annual review and completion of physical security information via MARMS by the Physical Security Officer or designated security representative on behalf of the DRO and field activities Director, DO, or SO. NOTE: Each DHA site, or facility AT Officer (ATO), Physical Security Officer, or designated security representative must have access to MARMS, via Secret Internet Protocol Router Network (SIPRNet), in order to review and complete the physical security (tab) portion. DHA tenants or GSFs coordinate with the host or parent DoD installation, if necessary, in order to conduct these assessments.

(1) The self-assessment review or evaluation include the following:

(a) Physical Protective Measures and Systems.

(b) Security Processes and Procedures.

(c) Assigned DCA, TCA, Tiered Assets, and other PL resources.

(2) Once completed, the Physical Security Officer or designated security representative notifies the respective DRO and field activities office, and DHA Protection Operations the information is available for review.

b. DRO and field activities Physical Security Officer or designated security representative will conduct a Physical Security Program Review annually on behalf of the Director, DO, or SO.

(1) The assessment will assess operability, identify gaps in operational procedures, refine policies, and create recommendations for program advancements, and will include:

(a) Access Control (Physical Access Control System (PACS)), Access Credentials, Keys, and Media Management).

(b) Intrusion Detection System (IDS).

(c) Closed Circuit Television or other related systems.

(d) SOP or Physical Security Plan.

(e) Security Incidents.

(f) Training, Drills, and Exercises.

(g) Facility Security Committee.

(2) The results of the internal program review, to include MARMS self-assessment, will be documented via memorandum, signed by the respective DRO and field activities Director, DO, or SO, and submitted via Non-classified Internet Protocol Router Network to the respective DRO and field activities Director or Designated Security Representative.

c. Conduct assessments of physical security infrastructure, systems or measures using applicable DoD-approved benchmarks, Interagency Security Committee (ISC), and Unified Facilities Criteria (UFC) standards, as well as guidance from the GCC or host installation in which the DHA sites or facilities operate.

d. The DHA Protection Operations assessment team or individual members of the DHA Protection Operations staff will conduct physical security assessments triennially. The DHA HQ will coordinate with each respective DRO and field activities office to establish a schedule and identify personnel to assist with conducting the assessments.

e. When possible, conduct physical security assessments in conjunction with vulnerability assessments (Reference (j)).

3. SECURITY DEFICIENCY AND WAIVERS. A deficiency is a failure or inability to meet applicable minimum DoD, ISC, or UFC standards, guidance from the GCC, or DHA Physical Security Program requirements. Deficiencies normally result in a higher security program risk. The security waiver process formalizes security program risk acceptance when deficiencies cannot be immediately corrected, and must be initiated by DRO and field activities Director, DO, or SO.

a. Purpose of the Waiver Process – The waiver process enables DRO and field activities Director, DO, SO, and DHA HQ to review, monitor, plan, and program corrections to deficiencies from approved guidance. The ultimate goal of the process is to ensure correction of all security deficiencies as quickly as possible or employ mitigating measures to reduce risk.

Waivers must be formally reviewed and updated annually by the DRO and field activities Director, DO, or SO, in coordination with the host installation if DHA is a tenant.

b. There are two types of waivers: Temporary and Permanent.

(1) Request a temporary waiver when compliance with a prescribed minimum standard is not currently achievable, and the deficiency is correctable within three years. Describe mitigating measures. Temporary waivers are granted when corrective action of a security deficiency is beyond the capability of the organization; or the deficiency can be corrected within three years. Submitted and approved temporary waivers, to include annual reviews, must be retained on file.

(2) Request a permanent waiver when compliance with a prescribed minimum standard is not achievable and is not correctable within 3 years. Justification must clearly explain why the standard cannot be met and why correcting the deficiency is adjudged not to be feasible or cost-effective after a critical evaluation of the facts and describe mitigating measures. Incorporate formally approved permanent waivers into security plans. Retain submitted and approved permanent waivers and annual reviews on file.

c. DRO, field activities, and DO or SO, as the subordinates of DHA HQ, manage the waiver process within their assigned facilities. DHA HQ has overall responsibility for the E-W management of the waiver process, in close coordination with DRO and field activities Director and DO or SO staffs.

d. In Reference (k), Commander United States Northern Command delegates to Defense Agencies authority to approve waiver requests from subordinate organizations in the USNORTHCOM area of responsibility. The DHA Chief of Protection Operations is the approving authority for waivers from established requirements within this publication. NOTE: DHA Chief of Protection Operations may delegate waiver authority, in writing, on an as-needed basis, one echelon lower.

e. Document security deficiencies on DHA Form 238, Request for Waiver from Security Criteria, and submit each waiver request for formal approval via SIPRNet. NOTE: Based on the long-term nature of permanent waivers, they should be incorporated into the AT and Facility Security Plan to codify risk acceptance and to formalize them as security planning factors. NOTE: Physical Security Officers and ATOs should ensure security waivers are also identified and captured in MARMS. Submitted and approved waivers, to include reviews, must be retained on file.

(1) Requestor or Initiator (DRO and field activities Director) will complete blocks 1 thru 17 (sign block 16); forward the document to the respective DRO or field activities Director (or security representative) for coordination or review via SIPRNet. DO or SO will submit the document directly to DHA HQ via SIPRNet. Do not submit waiver requests via non-classified Internet Protocol Router Network.

(2) DRO or field activities Director (or security representative) will review and provide comments as necessary as the Reviewing Official. Reviewing Officials note whether compensatory measures are considered adequate and, if not, specify additional measures. Additionally, Reviewing Officials make a recommendation to the Approval Authority and add amplifying information, as appropriate. Fill or sign blocks 18 thru 22, as the Reviewing Official, and forward the package to DHA HQ via SIPRNet.

(3) Waivers are routed and reviewed through the J34, Chief of Protection. The first flag officer or SES in the J34 routing chain approves or disapprove waiver requests, provide comments and rationale for the decision as necessary, fill or sign blocks 23 thru 28, and return the package to the Requestor via SIPRNet; courtesy copy the DRO or field activities Director if applicable.

(4) Based on the long-term nature of permanent waivers, Physical Security Officers and ATOs should be incorporated into the AT and Facility Security Plan to codify risk acceptance and to formalize them as security planning factors.

(5) Physical Security Officers and ATOs should ensure security waivers are also identified and captured in MARMS. Submitted and approved waivers, to include reviews, must be retained on file.

f. Every effort should be made to correct deficiencies that exist. A waiver request should not be made simply to save effort in securing a site, facility, asset, or personnel or for convenience purposes.

4. RESTRICTED AND CONTROLLED AREAS

a. Overview - This paragraph outlines procedures, authority, and responsibilities for establishing and maintaining restricted and controlled areas. Physical security requirements for restricted or controlled areas are identified in paragraph 8 of this Enclosure. Each military installation has an IDP or ISP which forms the foundation for installation defense operations. Each installation possessing or routinely supporting DCA, TCA, Tiered Asset, or PL resources must have an IDP or ISP. Additionally, DHA sites and facilities located off military installations must have a Physical Security Plan. NOTE: DHA sites and facilities located on military installations will follow host-installation guidance and procedures for establishing their restricted and controlled areas.

b. Authority - Reference (e) authorizes military commanders to issue guidance to safeguard property or places subject to the jurisdiction, administration, or in the custody of the DoD. The DHA delegated that authority in Reference (j) to DRO and field activities Director, DO, or SO. This gives them the authority to establish restricted and controlled areas for the protection of resources and personnel. For locations outside continental United States (OCONUS), ensure any guidance that applies to non-U.S. military or DoD civilian, or contractor personnel is consistent with any host-nation agreements, such as a Status of Forces Agreements.

c. Restricted Areas - Restricted areas are defined as an area under DoD jurisdiction in which special security measures are employed to prevent unauthorized entry. Restricted areas are normally assigned to protect assets for which the loss, theft, misuse, compromise, damage, or destruction results in mission degradation to the war-fighting capability of the U.S. Host Installation Commanders or DRO and field activities Director, DO, or SO approve designations for restricted areas and identify their location in the host-installation IDP, ISP, or facility's Physical Security Plan. DRO and field activities Director, DO, or SO will coordinate with the host DoD installation to identify and establish restricted areas within their facilities. Only designated personnel, authorized in writing by the responsible Director, DO, or SO will have access to restricted areas. Security personnel will remove access permissions for unauthorized staff and visitors and conduct quarterly system reviews to ensure that access to restricted areas is limited to authorized personnel. NOTE: The level of security for restricted areas must result in significant deterrence against hostile acts. Failing the ability to deter, defensive measures will ensure a significant probability to detect and defeat a hostile force before it is able to seize, damage, or destroy resources. Owners and users of resources within restricted areas must be actively involved in the security of their assets. Security response is provided by either the host-installation; facility security guards; or civilian law enforcement. When establishing restricted areas:

(1) Consolidate resources of similar assets for efficient use of available security personnel and resources, consistent with operational requirements.

(2) Clearly mark the boundary of each restricted area.

d. Controlled Areas - Similar to restricted areas, controlled areas contain resources that require specific security measures to prevent unauthorized entry. Controlled areas are normally assigned to protect DHA assets that directly or indirectly support DHA facilities and the war-fighting mission and which loss, theft, misuse, compromise, or destruction of which would adversely affect mission capability (e.g., pharmacies, medical logistics vaults, areas where large volumes of classified material are processed [Secured Room or Open Storage], areas storing Biological Select Agents and Toxins (BSAT), backup generators, fuel storage tanks, etc.). Installation Commanders or DRO and field activities Director, DO, or SO approve designations for controlled areas, which are defined areas containing resources or functions in areas with owners or users being responsible for security. DRO and field activities Director, DO, or SO will coordinate with the host DoD installation to identify and establish controlled areas within their facilities. Controlled areas are identified in the IDP, ISP, or facility's Physical Security Plan. Only authorized personnel, designated by the responsible Director, DO, or SO will have access to controlled areas. Security personnel will remove access permissions for unauthorized staff and visitors and conduct quarterly system reviews to ensure that access to controlled areas is limited to authorized personnel. The designation "controlled area" carries the same legal restrictions as a physical barrier. Unless physical barriers are employed, the actual effectiveness of securing a controlled area may depend entirely on the security awareness of the people working in it. When establishing controlled areas:

(1) Properly mark the area boundary and keep entrances to the minimum necessary for access and circulation control, safety, and security. The host-installation IDP, ISP, or facility's

Physical Security Plan designates permanent controlled areas by building number or name of the area involved. Properly post and clearly define all controlled area boundaries.

(2) Controlled areas may be established within restricted areas and vice versa.

(3) If an area is designated as a temporary controlled area, the Host Installation Commander or DRO and field activities Director, DO, or SO specifies in writing the period of designation. Mark the boundary with temporary boundary markers and warning signs. Consider the use of physical safeguards (e.g., Entry Control Points [ECP]) or locks) during non-duty hours if feasible.

(4) Any physical changes to a controlled area (e.g., transfer of ownership, downgrading the status, modifying boundaries) will be coordinated with and approved in writing by the Host Installation Commander, DRO and field activities Director, DO, or SO.

e. Not all areas qualify for controlled area status. DRO and field activities Director, DO, or SO should consider the following when requesting to establish a controlled area:

(1) Criticality to mission accomplishment.

(2) Resource location and current threat assessment.

(3) Number and clearance level of personnel requiring access.

(4) Existing internal security, physical safeguards, and floor plan.

(5) History of losses, damage, or theft.

(6) For new construction projects, Financial Operations (J-8) Facilities with the assistance of the Logistics Contracting office, J-34 Protection Operations, and host installation, as appropriate, will ensure all security requirements are addressed in the construction plan to include alarms that annunciate or link to existing systems, forcible entry resistance, and entry and circulation control.

(7) If the facility is an existing structure, DHA J-8 Facilities, along with the local civil engineering (or equivalent) office will determine whether the facility meets the necessary structural requirements for the proposed controlled area. NOTE: Record and retain these assessments.

5. SECURITY INCIDENTS. DHA personnel are responsible for reporting all suspicious activity or physical security incidents immediately to their security representative, their supervisor, or their DRO and field activities Director, DO, or SO. Failure to report security incidents may result in administrative or disciplinary action.

a. Suspicious activity and security incidents are defined in Reference (l), and may include, but are not limited to:

(1) Unauthorized access to DHA classified information, computer systems networks, sites, facilities, or space.

(2) Unidentified or unauthorized individuals lurking or trying to gain access to restricted or controlled areas.

(3) Unusual and disruptive behavior, aggression, hostility, etc.

(4) Unusual questioning or elicitation about personal or professional information from unknown sources.

(5) Receipt of e-mails or phone calls from unknown sources wanting personal or professional information.

(6) Workplace violence to include active shooter, threats, harassment, bullying, etc.

(7) Surveillance by unknown individual videotaping or taking pictures of facilities and personnel.

(8) Suspicious vehicles.

(9) Unattended bags.

(10) Personal safety issues concerning outside threats like former relationships that may be a potential risk to oneself or others.

(11) Espionage, sabotage, terrorist threats, or bomb threats.

(12) Theft or intentional damage to government property.

(13) Discovery of or possession of prohibited weapons as defined and listed in paragraph 7 of this enclosure.

b. Regarding suspicious activity and incident reporting, observant occupants and guard forces are the first line of defense against threats but may fail to recognize or report behaviors of significant security concern when they lack training about clearly defined indicators. ATOs must ensure initial and periodic security training addresses how to recognize suspicious and reportable behavior, based on the local threat.

(1) DHA sites and facilities located on DoD installations will report all suspicious activity, to include security-related incidents to the site or field activity Dispatch or Security Control Center; or host-installation security or law enforcement immediately if no dispatch or control center exists. NOTE: 9-1-1 should be utilized if no other emergency number exists for your installation. The

Dispatch or Security Control Center will then contact the host-installation law enforcement, who will respond, conduct all investigations and up-channel the report through the respective Installation Command Post in accordance with the appropriate Situation Report and Operational Report category (i.e., Operational Report 3) and procedures specified by Reference (m), or otherwise directed local procedure. DRO and field activities Director, DO, or SO should identify, coordinate, and establish additional support requirements via installation support plan, memorandum of agreement, etc., with host or parent DoD installations.

(2) For GSFs located off DoD installations, any threat indicators, suspicious activity, or security-related incidents need be reported to the site or field activity Dispatch or Security Control Center, security guard or Designated Security Representative immediately. NOTE: 9-1-1 should be utilized for any emergency situation. Dependent upon local installation support plans, memorandums of agreement, etc., the Dispatch or Security Control Center, on-duty security guard, or Designated Security Representative will then notify the Federal Protective Service, local or parent host-installation law enforcement concerning the incident.

(3) DRO and field activities Director will make reports to DHA in accordance with Reference (n) and complete DHA Form 260, Notice of Security Incident, concerning all security-related incidents to supplement notification requirements IAW reference (n).

(4) Once completed, submit DHA Form 260 to DHA Protection Operations at: dha.physec@health.mil within 24 hours of the incident. Coordinate with and inform intermediate organizations as appropriate.

(5) The subject of the e-mail submission should be listed as "SI" (Security Incident) and include the Facility and the date the incident occurred (e.g., SI – DHHQ – 20220514).

6. ACCESS CONTROL PROCEDURES. DRO and field activities Director, DO, or SO and their assigned Physical Security Officer will assess, identify, and establish the minimum number of entrances to DHA sites and facilities, necessary for access and circulation control, safety, and security. Use this information to develop Access Control Points (ACP) and procedures for personnel entering and exiting DHA sites and facilities through specific sets of doors, such as main entrance or emergency room doors. Standards for access to DHA space are promulgated in References (d) through (h) and executed according to the following:

a. Authorized Credentials - In accordance with References (d) and (o), the DoD Federal Personal Identification Verification (PIV) credential, the common access card (CAC), will be the principal identity credential for supporting interoperable access to DHA facilities, buildings, and controlled spaces. All PACS utilized by DHA sites and facilities must be able to grant access via the CAC. Security personnel will remove access permissions for unauthorized staff and visitors and conduct quarterly system reviews to ensure that access is limited to authorized personnel.

(1) DHA sites and facilities, based upon unique mission requirements, may develop, and utilize badges that do not comply with Reference (p) in order to complement access control for

identification (ID) purposes only (e.g., Access to Birthing Center or Hospital Maternity Ward, etc.).

(2) As a baseline, all DHA sites will have a visitor control process and distinctive visitor badges that clearly indicate whether escort is required. Patients and their visitors at treatment facilities will not normally be required to wear ID except in certain sensitive areas or at increased Force Protection Condition (FPCON) levels, at the discretion of the facility director or in accordance with AT and physical security plans. Treatment facilities will ensure their visitor process is in compliance with The Joint Commission guidance. DHA sites and facilities will have a plan to identify 100% of personnel entering the facility during elevated FPCON levels and as otherwise directed by DHA, the local installation commander, or the facility commander/director.

(a) Report lost, missing, or stolen badges immediately to facility security guards or the designated facility security representative.

(b) ID cards or 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 facility security guards or the designated security representative.

(3) Codify any use of badges or other ID cards that do not comply with Reference (o) in a local SOP, Physical Security Plan, or similar document.

b. ID Check and Vetting Procedures - Background checks authenticating an individual's identity and determining their fitness is a core principle of access control. Identity proofing is the process of providing sufficient information (e.g., identity history, credentials, and documents) when attempting to establish a person's identity. Individuals must appear at the host-installation Visitor Control Center or DHA security office to be identity-proofed and vetted. NOTE: Personnel not able to be properly vetted may not be granted unescorted access to DHA sites or facilities.

(1) A valid and unexpired driver's license or ID card issued by a State, provided it contains a photograph and biographic information such as name, date of birth, gender, and address, may be used for proofing and vetting purposes. ID will be physically proofed (hands-on), cross-checked, and validated against authoritative databases. Additionally, a Federal, State, or local Government-issued ID card may be used provided it contains a photograph and biographic information such as name, date of birth, gender, and address.

(2) Background criminal history checks are mandated for all unescorted personnel requesting or requiring access to DHA sites or facilities for official business and not for medical treatment. This applies to anyone who is 16 years of age and older. This must include checks of the National Crime Information Center, Interstate Identification Index, terrorist screening database, National Crime Information Center National Sex Offender Registry, and Justice Department National Sex Offender Public Website. For foreign contracts, additional checks such as the Department of Homeland Security E-Verify, U.S. visit and DoD Foreign Visit System-Confirmation Module may be required. Contracts must include the requirement for this

check in the statement of work. Facilities will coordinate with DRO, and field activities or DHA Protection Operations as needed for executing this function.

c. Authorized Escorting - Escort authority is limited to personnel with a current Federal PIV credential (e.g., CAC).

(1) Escort authority is inherent to all DoD military and civilian personnel with possession of an authorized access credential. Minors are not authorized to escort adults within DHA sites or facilities. NOTE: Foreign nationals may not be escorted at any time into a DHA site or facility without proper vetting through the appropriate DHA and host or parent DoD installation Foreign Disclosure Office (FDO).

(2) Host Installation Commander or DHA owner or user of the area will apply References (d) through (h) to determine eligibility for escorting personnel in restricted and controlled areas.

d. Authorized Sponsoring - DoD military and civilian personnel with possession of an authorized access credential (e.g., CAC) have authority to sponsor guests and visitors. DRO and field activities Director, DO, or SO will develop specific procedures for sponsoring guests and visitors, ensure this information is codified in a local SOP, Physical Security Plan, or similar document.

e. Unescorted Access to DHA Facilities or Controlled Space - Access to DHA facilities and controlled space is granted utilizing the CAC via PACS. All DHA personnel assigned to their respective site or facility are authorized unescorted entry and access. NOTE: Unescorted Access is limited to the specific floors or areas where the individual is assigned to perform their duties.

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

(a) DoD CAC.

(b) U.S. Government-issued, authenticated Federal PIV credentials.

(2) Other personnel requiring regular access to DHA space, who, due to the nature of their work, have not been issued a CAC or Federal PIV, may be authorized to obtain a local alternative badge as outlined in the local site-specific physical security SOP, Physical Security Plan, or similar document. Alternative access badges must have an expiration date and duty hours or times assigned to the credential, and the holder of the credential must provide a valid ID card, as well as be properly vetted.

(3) DHA personnel and visitors will display their DHA ID card or badge (if utilized) or visitor badge at all times while in DHA controlled areas or space. Proper display of the DHA ID card or visitor badge is above the waist on the upper torso, attached to the outermost garment, so it can be easily seen by staff and security. DHA personnel are responsible for addressing other individuals they may encounter not properly displaying their ID card or visitor badge.

(4) personnel are required to utilize their CAC each time when entering DHA controlled areas. This security measure identifies authorized access on the PACS and is a physical security access control requirement. "Piggy-backing" and "Personal Identification Number sharing" are not authorized. Example: If an individual follows you through a door without using their CAC, remind them of this requirement and ensure they stop and use their CAC. If the individual does not have proper access, escort them immediately to the nearest security guard or security representative, or call for assistance if needed.

f. Escorted access to DHA facilities or controlled space: Escorted entry applies to individuals with official business to perform within a DHA controlled area who have not been granted unescorted entry or access. Hosts or sponsors are responsible for visitor control. Escorts (Host or Sponsor) will:

(1) Meet outside of DHA controlled areas and positively identify individuals requiring escorted entry.

(2) Monitor and track all visitors within their respective areas via locally developed sign-in sign-out roster or similar method. NOTE: At minimum, the roster should include the following:

(a) Individual's name (last, first),

(b) Assigned organization or directorate,

(c) Date and time of arrival,

(d) Printed name of escort, and;

(e) Date and time of departure.

(3) Ensure each visitor is briefed on their duties and responsibilities, while under escort (group briefings are permitted): "Sir/Ma'am, I am (state your name), your escort for this visit. Prior to entering this facility or DHA controlled space, I am required to brief you on security procedures and your responsibilities. While you are in DHA controlled space, you must be under escort by an authorized individual at all times. You must stay with your escort until you depart the area. If you are issued a visitor badge, you must visibly display it on the front of your outermost garment — above the waist — at all times. If you are stopped or challenged by security, you must obey all instructions. Do you have any questions?"

(4) Maintain positive control and constant surveillance of escorted personnel at all times while in DHA controlled space. The number of individuals an escort official can escort at one time is based on the known trustworthiness of the visitors and the ability of the escort to have reasonable control of the visitors. DRO and field activities Director, DO, or SO will develop specific procedures and ensure the information is codified in a local SOP, Physical Security Plan, or similar document.

g. Visitor control procedures follow.

(1) Visitors not possessing one of the acceptable forms of ID specified in this DHA-AI 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 facility or DHA-controlled space.

(2) Foreign national visitors not possessing a CAC or U.S. Government-issued Federal PIV credentials will be issued a "blue" escort-required badge.

(3) A visitor may not escort another visitor.

(4) A visitor badge will not be considered valid ID for access into DHA space.

h. Foreign nationals (visitors) - A "foreign national" is any person who is not a U.S. citizen or a person who is not a naturalized citizen. Persons with a U.S. "green card" are considered foreign nationals. They are lawful permanent resident aliens who have a resident alien registration card (Immigration and Naturalization Service Form I-551), commonly known as a 'green card,' retain their foreign citizenship, and must be considered "foreign nationals." The terms "foreign national" and "alien" are used interchangeably. A person with dual citizenship, who is a citizen of the United States, and another country may be treated exclusively as a U.S. citizen when in the United States.

(1) Coordinate Foreign Visit Requests through the DHA Foreign Travel Office, to include the host or parent DoD installation FDO if necessary.

(2) Foreign nationals with a valid CAC or Invitational Travel Order are not authorized to sponsor any guests that are not on their ITO, to include U.S. nationals.

(3) Apply the following procedures for non-official foreign visits or guests. Any foreign visitor or guest not on ITO, not documented in the Foreign Visit System and traveling to any DHA site or facility in an unofficial capacity (e.g., family members and friends, contractors, etc.) will coordinate through the DHA Foreign Travel Office, to include host installation FDO, 10 days prior to arrival.

7. PROHIBITED ITEMS. The items that are prohibited in Federal facilities include any item prohibited by any applicable Federal, State, local, and tribal law and/or ordinance, as well as firearms, dangerous weapons, explosives, or other destructive devices (including their individual parts or components) designed, redesigned, used, intended for use, or readily converted to cause injury, death, or property damage. The list provided in Reference (q) applies to all facility occupants, contractors, and the visiting public. Prohibited items will normally be removed from DHA sites as soon as practical and turned over to appropriate authorities for disposition.

a. The following items are examples of prohibited items in accordance with Reference (q) and, therefore, prohibited within DHA sites and facilities, including GSA-leased spaces:

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

(2) 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.

(3) 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.

(4) Any weapon, the possession of which is prohibited under the laws of the state in which the DHA site, hospital, or clinic operates.

(5) Mace, pepper spray, tear gas, tear gas gun, or other chemical spray designed for self-defense.

b. Exceptions may be made for weapons authorized for carry in the performance of duties including active law enforcement on duty, Security Guards assigned to DHA facilities, and Armed Forces members when authorized by law.

c. Firearms will not be carried inside behavioral health areas except when needed in the immediate performance of official police or security duties (e.g., defeating a violent attack). No further restrictions on the carrying of firearms in DHA facilities may be imposed on personnel performing official law enforcement or security duties.

d. Law enforcement and security officers are not permitted to carry weapons in any DHA facility for the purposes of personal appointments or while seeking other medical services. As an exception, those personnel otherwise authorized to carry weapons on the installation and currently on duty may, with prior coordination affirming their organization's approval, escort family members to appointments and pick up medication at DHA pharmacies. This exception does not apply to any behavioral health area.

e. In accordance with subsection 930 of Reference (r) and Part 102-74, Subpart C of Reference (s), ensure, "Federal law prohibits the knowing possession or causing to be present of firearms or other dangerous weapons in Federal facilities by all persons not specifically authorized by Title 18 of the United States Code, Subsection 930(d). Violators shall be subject to a fine and/or imprisonment in accordance with Subsections 930(a) and (b) and Title 41 of the United States Code, Part 102-74, Subpart C," or similar host-installation approved sign is posted for all areas or facilities subject to weapons prohibition. Warning signs are normally displayed at each entrance to an area so they can be easily read by persons approaching on foot or in a vehicle.

8. PHYSICAL SECURITY REQUIREMENTS. This paragraph describes physical security requirements for DHA restricted and controlled areas and equipment. NOTE: These standards must be applied to facility and equipment upgrades as well as to all new equipment and facility procurements. Planners will use UFC during the planning stages for construction of facilities. All federal buildings, to include GSA-leased facilities or space, must comply with ISC standards concerning physical security requirements. Planners may use data derived from Systems Effectiveness Assessments to mitigate vulnerabilities and justify equipment procurement or design of new facility construction. These standards require a compliance-based approach to security, which needs to be met to ensure DHA assets are protected accordingly.

a. Physical Security Terms follow.

(1) Warning Signs - Place warning signs so they are clearly visible to persons immediately outside the perimeter of posted areas. Place signs so as not to aid intruders in climbing fences and breaching barriers or boundaries. Translate signs into the host-nation language if in a foreign country, or in areas where languages other than English are predominant. Exception: Placement of signs at OCONUS installations must comply with host-nation agreements. Use accepted danger or warning symbols on signs in areas with widespread illiteracy. NOTE: DHA sites and facilities located on military installations will adhere to the installation's policy concerning warning signs.

(2) Barriers and Obstacles - Barriers and obstacles are designed or employed to channel, direct, restrict, delay, or stop the movement of an opposing force. Also, they impose additional losses in personnel, time, and equipment to the opposing force. Barriers and obstacles can exist naturally, be man-made, or be a combination of both. The construction of barriers and obstacles may require extensive engineer support, time, and materials. Planning for operations involving barriers and obstacles requires timely, continuous, and reliable all-source intelligence support. Placement of barriers and obstacles is coordinated through the host installation (if DHA is a tenant) or through J-8 Facilities and DHA Protection Operations to identify conflicts with mission requirements. Coordinate with host-installation or local law enforcement to obtain threat tactics, techniques, and procedures or possible COAs that could defeat barrier plans. Reference (t) provides additional information on barriers and obstacles.

(a) References (u) and (v) provide guidance on barrier employment.

(b) Barrier plans must be effective to stop active vehicle threats at ECPs and stationary vehicle threats at critical facilities. Barriers are usually formed around or tied into an existing terrain feature or man-made structures. Although there is little flexibility in positioning these large-scale obstructions, flexibility exists in selecting and designing those features that will be enhanced or reinforced. Place barriers to manipulate enemy movement in such a way that supports the commander's intent and scheme of maneuver. Barriers can be configured to detect or channel enemy movement and should be covered by weapon field of fire, when possible.

(3) Boundaries - Boundaries mark the legal and physical limits of installations, facilities, restricted and controlled areas, free zones, and National Defense Area. Barriers are the primary means to designate the physical boundary where the use of force, including deadly force, is

authorized. Barriers for boundaries range from painted red lines to dual chain-link fences. Additionally, post restricted and controlled area signs indicate the type of area in accordance with this DHA-AI.

(4) Fencing - A fence (or any other natural barrier that offers equivalent protection) serves as a legal and physical demarcation of the area perimeter. It provides an obstacle and limited delay capability that must be breached by an intruder. A breach of the barrier by anyone without authorization is evidence of malign intent. Since a fence serves as a deterrent to the casual intruder, and a legal definition of an area generally excluded to the public, it should be considered a primary aid for resource protection applications. Beyond these functions, a fence line or any other barrier that is not under constant observation by security personnel or owner or user personnel, or equipped with an IDS, has very limited utility.

(5) Lighting - Carefully design interior and exterior lighting systems, including fixtures, lamps, primary and backup power, control components, and wiring. Coordinate closely with host installation's Civil Engineer (or equivalent) office and Physical Security representative on each phase of lighting projects to meet all requirements, such as illumination levels, uniformity, color rendering, and energy conservation.

(a) Special Design Considerations - Each element of a lighting system is placed so an intruder cannot defeat the lights by simply turning them off or cutting a power supply. Use lighting circuits designed to ensure failure of one or more lights does not affect the remaining lights.

(b) Replacing Lights - The using agency is responsible for identifying defective or burned out lights. The user will replace these lights or notify the appropriate installation Civil Engineer (or equivalent) office, J-8 Facilities, or Leased Facility Management Office within 24 hours for repair.

(c) Placement of Lighting - Ensure lighting systems that provide personal assessment capability and support immediate visual assessment (IVA) cameras are installed correctly. The placement of lighting should enhance assessment capabilities and prevent blind spots and washouts that could detract from assessment capabilities. Furthermore, access to lighting controls by security personnel and response forces is a vital element to the overall defensive posture of the DHA facility or restricted area. A well-lit area may be necessary to detect a threat; other times, the lights may need to be turned off to aid security and response forces in defeating an adversary. The IDP, ISP, or facility's Physical Security Plan will address when and if lights should be turned off in certain areas.

(d) Types of Lighting Systems - Depending on the location and type of resource to be protected, five basic lighting systems may be used. Often a combination of two or more types is necessary. Before determining the type of lighting system to be installed, analyze background shading and coloring differences. Dark backgrounds require more illumination than light-colored surfaces. There may be local restrictions that impact lighting due to effects on wildlife, observatories, etc. Include legal and facility engineering experts when planning changes to lighting systems.

1. Area lighting is designed to illuminate the area within the fence or boundary or illuminate the exterior of a building to enhance visibility.

2. ECP lighting allows an EC to see and recognize persons at some distance approaching the entry point. The ECP lighting also supports the EC's ability to check ID credentials, inspect vehicles and hand-carried items, etc. Determine locally the lighting needed when the ECP is unmanned.

3. Boundary lighting is usually required when the resource to be protected justifies boundary fencing. Boundary lighting covers the area outside the fence or physical barrier so that it will not only expose anyone approaching the area but also limit or restrict the vision of anyone outside the area trying to look in.

4. Special purpose lighting may include portable lights, spotlights, searchlights, or ballpark lights.

(6) IDS refers to systems protecting DHA resources within restricted and controlled areas. Notably within the Services, operational war-fighting assets have higher standards for IDS than others; however, the IDS standards for SCIFs and Special Access Program Facilities (SAPF) must meet the requirements in References (v) and (w), regardless of their status. NOTE: The requirement for IDS administrators only applies to SCIFs and SAPFs. Additionally, Reference (x) indoctrination requirement only applies to SCIF and SAPF IDS administrators with the level of access outlined in Reference (x).

(7) The term Intrusion Detection Equipment is used when referring to individual pieces of IDS equipment (i.e., one motion sensor as part of an entire IDS system).

b. PACS Requirements - DHA utilizes biometric, electronic, or mechanical technological security systems to manage and control access to and within DHA controlled facilities, spaces, etc.

(1) Procuring PACS - DHA Protection Operations, through the respective DRO or field activity, manages centralized procurement of PACS in support of DHA facilities. Most, if not all, DHA sites and facilities already have and are utilizing PACS that were originally procured by their former, responsible Service. Procurement and sustainment of PACS E-W is a coordinated effort. Therefore, coordinate all PACS procurement requests through the DRO or field activity Director, prior to submitting to DHA Protection Operations.

(2) Program funding begins at the DHA facility. DHA Protection Operations, in coordination with the respective DRO or field activity Director and host installation, defines specific requirements and programs for installation of new systems. DHA Director, J-3 helps advocate security funding for system life cycles and upgrades as necessary. Among all other funding concerns, particular attention needs to be paid to programming the costs involved in allied support and the potential for increased program cost growth based on infrastructure age.

(3) DHA Protection Operations manages and coordinates with host installations concerning PACS procurement and logistics consistent with established priorities and funding.

(4) In accordance with References (d) and (o), the DoD Federal PIV credential, the CAC, will be the principal identity credential for supporting interoperable access to DHA facilities, buildings, and controlled spaces. All PACS utilized by DHA sites and facilities must be able to grant access via the CAC. Security personnel will remove access permissions for unauthorized staff and visitors and conduct quarterly system reviews to ensure that access to controlled areas is limited to authorized personnel.

(5) DHA sites and facilities, based upon unique mission requirements, may develop, and utilize badges that do not comply with Reference (p) for ID purposes only (e.g., Access to Birthing Center or Hospital Maternity Ward, etc.). NOTE: The use of badges that do not comply with Reference (p) will be codified in a local SOP, Physical Security Plan, or similar document.

(6) Existing legacy PACS will continue to operate until upgraded or replaced with standardized, compliant systems. Operating maintenance costs to existing PACS must be balanced and justified against use of such funds toward transition to systems that comply with References (o) and (p).

(7) DRO and field activities Director, DO, or SO are responsible for managing all access credentials (cards or badges), to include individual and master hard-keys for accessing all interior and exterior doors of DHA facilities or controlled spaces according to this DHA-AI.

(a) DHA security guards, Physical Security Officers, or designated security officials will be responsible for accountability, management, issue, and turn-in of all access credentials, to include individual and master hard-keys to exterior and interior doors of DHA facilities or controlled spaces.

(b) Conduct a complete inventory of access credentials, keys, and other access media biannually.

(c) Outline specific key control procedures in a local SOP, Physical Security Plan, or similar document. Include guidance on coordinating key changes with the local Facility Management office, and identifying lost keys and cost associated with a lost key as the responsibility of the individual entailing an investigation of property loss.

(d) Although management of key control programs is a security responsibility, as a best practice there may be facilities, particularly those that have no security staff office or desk, where the keys can be maintained, issued, and received, by an occupant of that facility, with oversight by security personnel. This can provide more responsive service to building occupants as an alternative to keys being kept, issued, and received solely by security personnel in a separate facility.

c. IDS Requirements - IDS provides an electronic means of accomplishing area intrusion detection, alarm reporting and display, remote alarm assessment, and alerting security personnel to intrusions in order to enhance the protection of resources and facilities. Other security tools, such as fencing, lighting, and communications systems, complement IDS and provide security response forces an essential technological advantage. IDS can increase the effectiveness of security response forces in deterrence, detection, and warning. Posted warning signs or visible sensors can enhance deterrence. IDS detects intruders and warns security response forces of intrusions by annunciating an alarm at the host-installation law enforcement or security control center or alarm monitoring facility. IDS also provides a tool for security personnel to locate and assess the threat once detected and allow security response forces to rapidly respond to defend assets and either defeat or delay attacks.

d. Procuring IDS: Host installations have programs in place concerning the procurement, installation, deployment, and logistics support of their IDS. Testing, approving, and procuring IDS is a coordinated effort where DHA organizations are tenants. Therefore, all IDS procurement requests will be coordinated through the DRO and field activities Director and DHA Protection Operations prior to coordinating with the host installation.

(1) Program funding begins at the DHA facility. DHA Protection Operations, in coordination with the host installations, defines specific requirements and programs for installation of new systems. DHA Director, J-3 helps advocate security funding for system life cycles and upgrades as necessary. Among all other funding concerns, particular attention needs to be paid to programming the costs involved in allied support and the potential for increased program cost growth based on infrastructure age.

(2) DHA Protection Operations will assist facility and DRO and field activities Directors to manage and coordinate with host installations concerning IDS procurement and logistics consistent with established priorities and funding.

(3) IDS funding for controlled areas is the responsibility of the owner or primary user of the facility requiring the IDS. Use of commercially leased or purchased IDS is permitted; however, the IDS must meet or exceed all DoD standards. All requests for acquisition or modification of alarm systems is coordinated through DHA Facilities, DHA Protection Operations, and host installation before contract tendering. NOTE: Coordinate all purchases of commercial IDS with the host installation, Civil Engineer (or equivalent), and Communications offices to ensure compatibility.

e. Replacing IDS: The normal life of IDS is about 10 years. Plan to replace IDS accordingly. Each DRO and field activity will provide DHA Protection Operations with a semiannual system status report to help determine IDS health and scheduling of replacement. NOTE: IDS that is being replaced is required to tie into the existing on-installation annunciator in which all other alarms annunciate.

f. Restricted or Controlled area IDS requirements: DHA facilities should utilize Risk Management Process to determine the most cost-effective means of protecting assets. At minimum, establish a detection capability that will detect unauthorized personnel prior to

entering the restricted area. The location of the line of detection may depend on installation-unique design factors, commander's, or director's level of risk acceptance, "Mission, Enemy, Terrain, Troops, Time Available, Civil Considerations," etc.

(1) Area or facilities manned 24 hours a day are not required to have IDS. However, they must have a duress alarm that terminates at the host-installation law enforcement desk or local alarm monitoring facility responsible for dispatching response elements.

(2) All Primary Occupancy areas or facilities not manned 24 hours a day are required to have IDS. They must have a detection capability for all facility openings greater than 96 square inches that terminates at the host-installation law enforcement desk or local alarm monitoring facility responsible for dispatching response elements.

(3) For Secure Room and Open Storage (of classified materials), the certification approval authority is the servicing or host-installation Information Protection office. For SCIFs, the accrediting official must approve interior IDS before purchase and installation and is responsible for testing. For SCIFs, the IDS standards must meet the requirements in Annex B of Reference (w) and Reference (y), and the DHA Special Security Office must be included in the planning process. For more information on SCIF requirements, refer to Annex B of Reference (w).

(4) Where IDS is installed in a facility outside of a host installation and monitored by a local or commercial monitoring service, plans must be coordinated and developed with local law enforcement agencies for immediate response to activated alarms. Response agreements and requirements must be documented in applicable contracts and mutual aid agreements.

(5) Some DHA sites and facilities located on or off DoD installations have internal monitoring. Where IDS is monitored internally by DHA security guards or personnel, plans should be coordinated and developed with the host DoD installation or local law enforcement concerning response and notifications of activated alarms. Response agreements and requirements must be documented in applicable contracts and support or mutual aid agreements.

g. All permanent restricted areas must employ an IDS concept of operations that provides IVA of exterior alarms. Security response forces perform assessment in near-real time to determine the cause of an alarm and initiate an appropriate response. The period of time between notification of an event, such as an alarm, and the assessment of the event should be as close to instantaneous as possible.

(1) Assessment or surveillance is accomplished either by the IDS operator using electronic video imaging equipment or security response forces. Electronic imaging equipment provides assessment and surveillance functions which enable the operator to conduct visual observations during alarm and non-alarm situations.

(2) Assessment occurs when imagers that provide near real-time video coverage associated with an alarm condition or sensor activation are used. Operators utilize assessment

devices to conduct IVA of alarmed sectors and direct response forces to potential threats within the area. Assessment devices can encompass analog or digital systems.

(3) Surveillance occurs when imagers are used to provide near real-time video coverage not associated with alarm condition or sensor activation. Surveillance devices can encompass analog or digital systems.

(4) Security response forces must be dispatched immediately when the IDS operator cannot determine the cause of an alarm via IVA or posted security guard.

h. Posting IDS warning signs - For all areas or facilities protected by IDS, ensure, "Warning-This Facility is Protected by Intrusion Detection Alarm System-Warning," or similar host-installation approved sign is posted. Warning signs are normally displayed at the boundary of each area and at each entrance to an area so they can be easily read by persons approaching on foot or in a vehicle. Maximum spacing between boundary signs usually do not exceed 100 yards. However, exceeding this distance may be necessary when placement of a sign is not feasible due to terrain features. Mark entry points of large facilities containing numerous IDS, as appropriate.

i. Unless otherwise specified within this DHA-AI or Higher Headquarters (HHQ) guidance, the owner or user must test IDS quarterly.

(1) IDS testing for Arms, Ammunition and Explosives (AA&E). In accordance with Reference (z), AA&E facilities' (e.g., armories) IDS will be tested monthly to ensure the proper functioning of the alarm sensors.

(2) Document such tests in a log and retain for one year active and one year inactive to monitor trends.

(3) The owner or user will designate, in writing, personnel responsible for IDS testing and will develop a testing schedule for the area or facility. Develop the plan with the assistance and approval of the host DoD installation ESS PM (or designated representative).

j. All DHA Divisions, Branches and Sections required to operate IDS due to resource requirements or DHA HQ guidance must follow these requirements:

(1) Specify in writing to the host or parent DoD installation or local alarm monitoring center who may activate or deactivate alarm systems and who may pick up authentication codes.

(2) Ensure the letter is current by updating personnel changes.

(3) Post owner or user personnel to guard the area if the IDS fails or is determined to be unreliable by the host or parent DoD installation ESS PM or local alarm monitoring center designated point of contact.

k. Restricted and controlled area physical security measures - A Risk Management Process of the installation determines if the additional security measures are needed to defeat adversaries. The desired effects of security for restricted areas include the ability to deter adversaries by proper marking and circulation control. The ability to detect threats is accomplished through proper ID of persons inside and outside the restricted area. Assessment is achieved through proper detection of unauthorized or suspicious persons or activities in and around the area. Personnel working within restricted areas can provide the, "warn," capability by observing and reporting suspicious activities or persons to security response forces. Delay is achieved through a robust security presence and placement of physical security measures commensurate with the asset being protected. Furthermore, restricted areas ensure the asset is defended to the greatest extent possible through proper design, controls, and employment of procedures.

(1) Many DHA sites and facilities are located on military installations. In addition, standards of protection, in order to meet these desired effects, differ substantially in numerous ways (e.g., signs, boundary requirements, fencing, barriers, gates, circulation control, lighting requirements). However, despite these differences, providing an adequate level of security is the overall goal and can be achieved by a standards from the host Military Department.

(2) Regarding physical security requirements for restricted and controlled areas, DHA facilities will:

(a) Follow and adhere to host-installation physical security requirements.

(b) Coordinate with the DRO and field activities Office (and DHA Protection Operations when needed) to resolve any conflicts or disputes relating to physical security matters.

l. Firearms of all types are susceptible to theft. Certain military-unique firearms, because they are unavailable on the commercial market and their potential to cause great numbers of casualties are particularly susceptible. All DHA facility Director, DO, or SO and supervisors, therefore, must place special attention and emphasis on protecting firearms. To reduce theft vulnerability and protection costs, Directors, DO, or SO, must closely scrutinize the number and location of all firearms storage facilities or areas within their assigned facilities with the goal of reducing and consolidating wherever possible, consistent with operational, training, and safety requirements. This DHA-AI does not require creation of firearms storage capabilities not otherwise needed. Owners or users should only remove firearms from storage areas for as short a time as possible, and in the smallest quantity needed, to support specific functions or requirements.

(1) Return all government-issued firearms and ammunition utilized by on-duty security guards to a designated control point on completion of the assignment, for storage and accountability in an authorized storage facility or container per References (z) and (aa).

(2) Privately Owned Firearms will not normally be stored, within the DHA facility armory or weapons storage area or room. In exceptional circumstances such as urgent situations

or medical emergencies private weapons may be stored if kept separately such as a separate drawer or GSA approved container.

(3) DRO and field activities Director, DO, or SO, in conjunction with the DRO and field activities Director's office and DHA Protection Operations, will coordinate with the host-installation Physical Security Officer concerning firearms and ammunition storage within their respective facilities (e.g., identifying requirements and facility criteria, restricted or controlled area designations, IDS requirements, approving storage area or facilities).

(4) Physically inventory and account for all firearms, ammunition, and NLW in accordance with References (z) and (aa).

m. Pharmacies and controlled substance storage areas are lucrative areas for pilferage, burglary, and robbery. The pharmacy's lead medical officer or civilian employee will ensure that controlled medical items are properly stored and that storage areas meet the criteria in Reference (ab) for caged or vault storage space. Additionally, these areas must be protected in accordance with the Code of Federal Regulation guidelines (as listed below), in conjunction with host-installation guidance, as necessary. Designate these areas as restricted or controlled areas and include in the installation's resource protection program.

(1) Controlled substance storage areas must meet the security specifications outlined in paragraph 8.l. of this enclosure and Part 1301.71 through 1301.76 of Reference (ac).

(2) Controlled substances in medical logistics vaults or safes must be stored in compliance with the security specifications outlined in paragraph 8.l. of this enclosure and Section 1301.71 through Section 1301.76 of Reference (ac).

n. For the purposes of the BSAT Program within all DHA administrated facilities, all areas within DHA facilities registered with the Federal Select Agent Program in accordance with the requirements in Part 331 of Reference (ad), Part 121 of Reference (ae), and Part 73 of Reference (af), will be designated as a restricted or controlled area and protected as a critical resource. NOTE: DHA facilities will adhere to host-installation physical security requirements concerning restricted and controlled area determinations. Reference (ag) provides specific security requirements for BSAT facilities. Those BSAT-registered DHA facilities that do not regularly maintain a BSAT inventory (e.g., the Air Force Laboratory Response Network Reference Lab) will only apply this PL designation when the agents (or presumptive agents) are present.

o. Protect all Controlled Unclassified Information (CUI) and classified information in accordance with References (l) and (ah).

(1) Directors, DO, or SO will coordinate with their respective DRO and field activities Director, and host-installation information security office concerning minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for storing and protecting classified information.

(2) Comply with all physical security requirements concerning classified information identified in Reference (i).

(3) Comply with all physical security requirements concerning CUI identified in Reference (ah).

9. TRAINING AND EXERCISES

a. DRO and field activities Director, DO, or SO have broad flexibility to adapt physical security operations for local conditions. Physical Security operations may vary widely between locations. These variances create unique challenges in verifying accountability and validating operational proficiency and readiness.

b. Security guard supervisors should coordinate planning, tactics, and rehearsals with host-installation and local law enforcement (if partnered with via mutual aid agreement). Effective, realistic training through "force-on-force" exercises is manpower and resource intensive. Often DHA security guards are limited by local conditions from conducting all "mission-specific" training they most need. Computer-based training and simulator systems provide realistic training tools to supplement (rather than replace) live training and their use is highly encouraged. DRO and field activities Director, DO, or SO should make every effort to ensure those tasked with providing security response are familiar with and competent in security tactics, techniques, and procedures, such as responding to violent unarmed patients and armed active threat intruders.

c. A security exercise allows the DHA sites and facilities, as well as supporting forces, the ability to simulate FPCON and contingency actions they could not otherwise effectively practice during daily operations. DRO and field activities Director, DO, or SO will work closely with the host DoD installation emergency responders to conduct joint-security exercises. GSFs will coordinate and work closely with their parent DoD installation, Federal Protective Service, Pentagon Force Protection Agency, and local emergency services personnel to conduct security-related exercises.

(1) Conduct local exercises as frequently as needed to maintain a high degree of readiness. As a minimum, exercise at least one hostile threat scenario involving all DHA site and facility security and response forces annually. This exercise can be included as part of another required exercise (e.g., increased FPCONs, mass casualty, AT or Chemical, Biological, Radiological, or Nuclear [CBRN] attack). Design exercises so they will not impede mission essential activities or create hazards to health, life, and safety. Consider potential impact on patient care. Include the Public Affairs or Communications Office in planning for all facility exercises to reduce the likelihood of personnel confusing exercise events with actual emergencies.

(2) DRO and field activities Directors, Host or Parent DoD installation(s) and local DHA facilities identify the types of contingency actions to be exercised.

(3) DRO and field activities Director, DO, or SO will coordinate with host or parent DoD installation to develop specific training and annual exercise schedules. Exercises should test the physical security plan's established processes and procedures. Conduct exercises in accordance with locally established exercise, evaluation, and safety guidance. DRO and field activities Director, DO, or SO will make every effort to ensure maximum participation in exercises. NOTE: Scenarios should be designed to test effectiveness of security measures and systems in place. If the exercise provides compelling indicators of new vulnerabilities or the risk acceptance is inappropriate, the Physical Security Officer, or responsible official will present this issue to the DRO and field activities Director, DO, or SO and request revised guidance. This additional guidance should also be documented (e.g., update AT plan, EPRM, MARMS, etc.) and the planning process should be repeated.

(4) For annual exercises, members of the exercise evaluation team, in coordination with the host or parent DoD installation, should develop scenarios utilizing adversary tactics, techniques, and procedures that represent the specific threats to the installation or GSF. As a minimum, the exercise evaluation team will develop threat scenarios to test friendly plans against the most likely and most dangerous adversary COAs.

(5) Escalation to higher threat levels and FPCONs should be included as part of the exercise.

(6) DRO and field activities Director, DO, or SO will ensure an exercise evaluation is conducted and documented via After Action Reports (AAR). NOTE: If the host DoD installation is responsible for the AAR, DRO and field activities Director, DO, or SO will request and maintain a copy on file.

d. DHA HQ and each DRO and field activity should develop visit programs to meet their intent and needs as a HHQ or as requested by the DHA facility (e.g., inspection preparation, program review). DRO and field activities Director, DOs and SOs are highly encouraged to use these visits to identify and resolve problems and allow responsible installation agencies to join in planning and programming actions.

e. DHA HQ, in coordination with each DRO and field activity, will conduct triennial inspections of the facility Physical Security Program. Installation requirements that duplicate the criteria of DHA HQ inspections may be accepted as meeting the triennial requirement. This includes exercises conducted as part of HHQ evaluations.

10. ARMED SECURITY GUARDS. The protection of DHA resources (and in the case of defense critical infrastructure, task-critical assets in accordance with Reference (ai)) is best accomplished by careful integration of armed security guards, procedures, and complementary physical protective features and equipment, e.g., fencing, lighting, locks, and IDS.

a. Security guards responsibilities and equipment - DHA security guards are the enterprise leader for delivering armed security response capability; however, security guards are not the sole proprietors of DHA's security program. All DHA personnel must actively participate in the

defense of DHA sites and facilities, resources, activities, and missions. Directors of non-security guard personnel who have security responsibilities requiring specialized equipment, should consider programming for equipment compatible with local security guards to ensure seamless and mutually supporting capability between security guards and non-guard forces.

(1) Guard force composition and responsibilities – Security guards protect resources that directly support the DHA mission worldwide. On-duty security guard response elements are required for those DHA sites, facilities, compounds, or areas deemed necessary to provide an adequate level of security. They form a major part of the total capability for detecting, responding to, and neutralizing hostile actions under normal and emergency conditions. The number of required security guards may vary, based on the mission(s) they are required to execute. Members of each guard unit must know their individual responsibilities and must also have a working knowledge of all positions within their assigned site or facility. NOTE: Security guard manpower is determined by the number of required security posts and patrols. Security guards are NOT authorized to perform duties outside of their assigned duties and authority. Security guards may be assigned additional or special duties, per the direction of the DRO and field activities Director, DO, or SO and Chief of Guards, to support the mission of the DHA facility and ensure the safety and security of personnel and resources. These duties may only include inherently security guard related functions (e.g., access control, security patrol, ESS/IDS monitor, etc.) and be performed only in areas under the authority or jurisdiction of DHA.

(2) Shift Leaders ensure proper individual and collective training, equipping, conduct, and the welfare of the guards on duty. They must know each person assigned to the guard force, especially their strengths and weaknesses. They are also responsible for the basic operation and administrative functions of the shift.

(a) Shift Leaders are responsible for preparing and posting duty schedules and scheduling leaves.

(b) Upon arriving for duty, Shift Leaders will confer with the Shift Leader being relieved and receive a thorough briefing on the current status of security operations, or review logs if there is a gap between shifts. They will also check the status of vehicles, communications equipment, checklists, and any other equipment their personnel will need during their shift.

(c) Shift Leaders should check each post at least once during their shift.

(d) Shift Leaders are responsible for executing security operations and knowing the threats and any security gaps or vulnerabilities. They are also responsible for ensuring posted guard forces understand their role in overall security posture and operations.

(3) Supervisory Security Guards can perform and be assigned to various security positions, as deemed appropriate by the Shift Leader. Supervisors oversee and are responsible for conducting individual and collective training of the guard force. Training includes on-the-job and proficiency training requirements. Supervisors will supervise guards based upon site-specific “Mission, Enemy, Terrain, Troops, Time Available, Civil Considerations” factors;

thorough analysis of the security risk management process; and the guard force's ability to anticipate, deter, detect, assess, warn, defeat, delay, defend, and recover.

(4) Entry Controllers (EC) or Access Controllers (AC) control entry to specific locations within DHA administrated facilities (e.g., entrances to DHA sites, facilities, compounds, restricted or controlled areas, cordoned areas). They perform duties in some of the most sensitive positions as part of the security program. They must apply controls that ensure only authorized personnel are admitted to the areas for which they are responsible. This DHA-AI and local supplements contain the procedures ECs must follow in the performance of their assigned duties.

(5) Assistant EC or AC may be posted to conduct vehicle and personnel searches and assist the EC or AC as needed.

(6) Security patrol limits will vary by location depending on local installation and local law enforcement procedures and agreements. Patrols may operate inside or outside DHA sites, facilities, compounds, or restricted areas, administered by DHA. Security patrols observe assigned facilities, area, and resources and provide immediate response to alarms generated from IDS or personnel and incidents. Security patrols must be capable of responding immediately to any threat or emergency situation. NOTE: If approved by the DRO and field activities Director, DO, or SO, two-person security patrols may be separated and work as single-person security patrols within their assigned area(s) in order to facilitate area coverage and response to alarms.

(7) IDS monitors are required to monitor IDS systems. They may dispatch security patrols to alarms and may make initial incident notifications. Depending upon site, facility, and area configuration, they may control entry to alarmed facilities, areas within facilities, and other locations protected by IDS.

(8) Security Guard Dispatchers direct guard forces during normal and emergency security operations. Persons assigned to this position must be of the highest competence because of its demanding nature and critical duties. Dispatcher responsibilities include:

(a) Operating the communications console and equipment.

(b) Up-channeling reports.

(c) Plotting locations of all posts, patrols, and PL resources during emergency situations.

(d) Dispatching patrols and notifying posts during emergency situations requiring response or action.

(e) Completing required reports and other administrative duties.

(f) Making notifications to interested persons, as directed.

(g) Receiving 911 calls (if applicable).

(9) Commercial vehicle inspectors perform inspections of commercial vehicles entering the DHA sites, facilities, compounds, or areas under the authority and jurisdiction of DHA and complete paperwork associated with the inspections.

(10) Overwatch posts prevent the ingress of vehicles attempting to enter the DHA site, facility, or compound for hostile purposes.

(11) Visitor Control Center posts validate unrestricted entry to authorized personnel and determine visitor purposes for entering the DHA sites, facilities, compounds, or areas under the authority and jurisdiction of DHA. These posts issue visitor and vehicle permits, conduct ID credential inspections, and maintain records of debarred or restricted personnel.

b. DHA HQ will specify the type of weapons guard forces carry or delegate responsibility to DRO and field activities Directors, as necessary, recognizing that transition of weapon systems is phased over time. DRO and field activities Director, DO, or SO ensure guard personnel are armed and equipped to perform their assigned duties. The primary weapon(s) DHA guards will carry include the M17 handgun with three magazines loaded with 17 9MM ammunition rounds each (51 rounds total); along with an expandable baton and a TASER (electronic control weapon).

c. All on-duty security guards must be equipped with the following:

(1) Whistle - Whistles can be used to signal other guard members, signal persons, or vehicles to stop or to attract the attention of others in case of emergency.

(2) Flashlight - Security guards may need to enter a darkened area during daylight hours (e.g., interior of a facility, etc.).

(3) Cold and foul weather gear - Depending on climate, geographic location, and time of year, guards are recommended to the have appropriate cold and foul weather gear available on post. DRO and field activities Director, DOs, or SOs will codify any specific requirements in local guidance, not listed in this DHA-AI.

(4) Duty belt, harness, tactical vest, holster, handcuffs with key, restricted area badge, and ID card (i.e., CAC, ID badge).

d. Body armor and protective masks - DRO and field activities Director, DOs, or SOs, through their respective threat working group, will determine when protective masks will be worn or readily available and will ensure guards are adequately equipped with body armor to meet the higher threat of an active shooter situation to include availability of Type IV armor to defeat high velocity small-arm rounds.

(1) While protective masks (e.g., M50) are not normally used to respond to a CBRN incident during non-contingency postures, they can be used by guard personnel (both military and government civilian employees) during military unique operations (e.g., readiness training

exercises, home station defense during CBRN events, etc.). If protective masks are issued, all guard personnel must be trained on the use, maintenance, and operational limitations of the masks by their servicing Emergency Management office. Additionally, guard forces will consult with the installation or servicing Bioenvironmental Engineering office to determine if the mask is appropriate for local threats and its intended use. In cases where a specified protective mask is not appropriate for use, Bioenvironmental Engineering personnel, coupled with the Threat Working Group, will provide the DRO or field activities Director, DO, or SO a recommendation as to whether a more appropriate protective mask should be used. When a protective mask is not available or is deemed ineffective for the potential threat, procure protective masks certified by the National Institute for Occupational Safety and Health with guidance and approval from the installation or servicing Bioenvironmental Engineering office.

(2) Select concealable body armor when procured using the National Institute of Justice (NIJ) Consumer Product List as a guide. The NIJ Technology Assessment Program lists body armor models in their Consumer Product List that have been tested by the NIJ and found to comply with the requirements of Reference (aj). This standard can be found on the NIJ webpage https://www.nij.gov/topics/technology/body-armor/Pages/welcome.aspx. This change will provide end users of body armor a more comprehensive and complete listing of the myriad of concealable body armor types available that meet the NIJ standard as well as explain the standard and its supplement. Armor that complies with this standard meets the minimum performance requirements critical for protection. Reference (aj) specifies five levels of ballistic performance for body armor. The first three levels – IIA, II and IIIA – are typically soft armors. The two remaining levels, III and IV, are typically hard armor designed to protect officers against rifle threats. The minimum body armor protection requirement for all DHA security guards will be Type IIIA. This armor is sufficiently comfortable for full-time wear. DRO and field activities Director, DOs, or SOs must, based upon local threat assessments, ensure guards have the capability to transition to a higher-level body armor type (e.g., III or IV), as needed.

e. Night Vision Devices (NVD) - This is an optional item, which can be utilized by posts and patrols during hours of darkness. DRO and field activities Director, DOs, or SOs who identify an operational requirement to utilize NVDs will coordinate with their respective DRO and field activities Director's office, prior to requesting DHA Protection Operations approval. NVDs should be identified and selected via the Small Arms and Light Weapons Accessories List (e.g., AN/PVS-14, monocular). Replace existing older model NVDs through attrition. One set of NVDs per security patrol. NOTE: Two sets of NVDs if patrols are split to meet local security requirements.

f. When required as Security Patrols, guards will be authorized use of government vehicles to perform their assigned duties (e.g., escorts, area patrol, and routine or emergent responses). The vehicles will be DHA-owned or controlled transportation assets operated for official use only and managed in accordance with Reference (ak). Use of privately owned vehicles is not authorized for security guard mobile patrols. Security guards must have a valid and current permanent (i.e., no permits) driver's license issued by a state, the District of Columbia, Puerto Rico, or a territory or possession of the United States. Foreign national security guards must have a valid and current permanent driver's license from their respective host-country. Terrain and the intended use of a vehicle (e.g., for escort, area patrol, and routine response force

elements) should determine the type of vehicle best suited for a particular DHA-controlled site or facility mission.

(1) In areas of rugged terrain and areas subject to periods of heavy snow, rain, or adverse weather, a capability for off-road travel must be available to security guards. This requirement may be satisfied through use of four-wheel drive vehicles. NOTE: Vehicles should not operate off hardened surfaces unless absolutely necessary.

(2) All permanently assigned guard vehicles must be properly marked, "Security," and have public address systems, and (except where barred by local restrictions) sirens and amber or yellow emergency lights. Vehicle mounted radios are recommended, but communications may be maintained via hand-held radios. Security guards must be familiar with and trained on the use of all vehicle-mounted equipment. NOTE: When temporary vehicles are used, ensure they are properly marked with magnetic signs and equipped with portable emergency lights and public address systems.

(3) Specialty Vehicles - DRO and field activities Director, DOs, or SOs who identify an operational, AT, or Physical Security requirement to utilize specialty vehicles (e.g., All-terrain vehicles, Class I/II sport utility vehicles, Segway® Personal Transporter) will coordinate with their respective DRO and field activities Director's office, prior to requesting DHA Protection Operations approval. DRO and field activities Director, DOs, or SOs will develop process for sustainment and training for all special vehicles and equipment.

g. Security guard communication requirements - Of all supporting equipment and systems used in security operations, the security communications system is one of the most important. The ability to sound the alarm is directly impacted by communications systems. As an element of security operations, enabling the desired effects of detect, warn, and defeat, communications allow detected events to be reported to the DHA facility Dispatch or Security Control Center so friendly forces can be warned. Subsequently, unimpeded communications can enhance guard force effectiveness in defeating the threat. DHA security guards must have landline capabilities and radio net, with a minimum of two frequencies, or the system must allow the guards continuous communications during radio net meaconing, intrusion, jamming, or interference conditions.

(1) The telephone service provides lines for calling in and out of the DHA facility, connection of special (hot) lines, lines for fixed posts, and Defense Switched Network capability. Equipment of this type is relatively dependable and, as a rule, is less expensive than radio systems. However, the lack of mobility or portability limits their use to stationary security posts. Landline systems also include intercom systems, voice over internet protocol, and secure communications means such as Secure Telephone Equipment.

(2) DHA facilities must make the best possible use of systems that provide secure voice capabilities. Command and control (C2) radio system encryption must be commensurate with the level of information to be transmitted over them and be in compliance with National Security Agency-approved encryption standards. Type 3, Advanced Encryption Standard is the current National Security Agency-approved encryption for sensitive but unclassified information.

Provide land-mobile radios, base stations, and repeaters with an uninterruptible power source and to the greatest extent possible, the manual duress systems for hand-held radios should be enabled. Ideally, radios equipped with duress buttons display the radio's location graphically on DHA facility Dispatch or Security Control Center display terminals. Assign and issue radio frequency authorizations according to host or parent DoD installation or local civilian first responder frequency authorization guidance.

(3) Land Mobile Radio (LMR) system - Radios are the most versatile and effective security communication equipment. The radios used in connection with security operations include base stations, mobile two-way, and portable. There are many different brands and models currently in use throughout the DHA; however, planning considerations must include spectrum management for frequency deconfliction and, when possible, integration with local first responder trunked or otherwise encrypted LMR to allow for rapid communication and coordination during contingency operations. This can include P331 initiatives within the U.S. to share encrypted communications infrastructure between DoD and local, county, or state government agencies. Types of radios include:

(a) Base Stations: Fixed two-way radios, usually located in the DHA facility Dispatch or Security Control Center. All base stations should be provided with an emergency power source.

(b) Base Station Remotes: Fixed two-way radios installed on fixed posts. Remotes are basically amplifiers connected to the base station with telephone lines and use the base station to send and receive calls.

(c) Mobile Two-Way Radios: Usually installed in security guard vehicles. These radios can talk over great distances in dispersed situations. Some models can be easily removed from vehicles, making them mobile-portable radios.

(d) Portable Radios: Two-way radios, used on security patrols and fixed posts. These radios can talk over short distances and are used for most normal day-to-day operations.

(4) Provide radios to guard forces.

(a) Give each static post member a portable or fixed two-way radio.

(b) Equip each security vehicle used on a regular basis with a mobile or portable two-way radio.

(c) Install direct or hotline instruments at each permanent static post.

(d) Devise manual systems at each DHA facility to back up the LMR and landline systems.

(e) The DHA facility must back up the LMR system with a landline system.

(5) Certain procedural practices facilitate transmission and reception of messages. Guard forces using radio equipment must know these procedures.

(6) Each post and patrol issued a radio is assigned a call sign, that is a combination of letters and numbers, identifying the user without disclosing the user's name or location.

(7) All posts and patrols entities should use common terminology for communications. Standard common terminology is a key principle of the Incident Management System. Because of this, it is important to limit the unnecessary creation of terminology. While joint military communities utilize common pro-words, when responding in conjunction with civilian counterparts, care should be taken to minimize the use of radio pro-words. 10-Codes should not be utilized during radio communications.

(8) Clear speech: Keep the message short and use as few words as possible. Talk and speak clearly when sending and transmitting messages.

(9) Phonetic alphabet: Used when correct reception is critical, and words, abbreviations, or groups of letters are difficult to understand.

(10) Prohibited radio practices: The Federal Communications Commission prohibits certain things from being transmitted. Prohibited radio practices include the following:

(a) Profane or obscene language.

(b) Unnecessary, extravagant, false, or deceptive messages.

(c) Transmissions not in accordance with station license.

(d) Transmissions made by unauthorized operators.

(11) Backup systems: Landline and radio systems can be supported with the following:

(a) Recording capability for telephonic systems is no longer mandated by DoD; however, the capability generally exists within enhanced 911 systems. The laws of each state direct when telephonic systems can record. Security guard units, through their respective communications support agencies, branches, or divisions, must coordinate with the residing state and servicing DHA Office of the General Counsel attorney to ensure compliance with local laws and regulations for telephonic recording capability. Telephonic system recording must be extended into the DHA facility Dispatch or Security Control Center if recording is available and permitted. Field systems are tactical phone systems, normally manually operated and providing service to stations connected to the system. As an additional backup, cellular systems may be utilized so long as they are encrypted to the level of information that is communicated on them.

(b) During emergency situations where landline communications can become saturated, it is suggested that Government Emergency Telecommunications System priority access telephone cards be obtained from host DoD installation communication units or respective communications support agencies, branch, or divisions. This is a telephone card with a telephone number and Personal Identification Number that will give priority to the calling entity. Suggested card storage

locations for guard units would be at the DHA facility Dispatch or Security Control Center, Alternate location, or with the local Chief of Guards.

(c) Cellular Systems: These are mobile cellular telephones and associated support systems. Cellular systems should be used only for backup in case other telephonic systems fail. Additionally, cellular systems should be encrypted to the level of information that is communicated on them. DHA J-6 and host DoD installations will provide guidance on cellular use restrictions.

(d) Voice: This method is common to all personnel. The tactical situation, language abilities, and distance between the person talking and the person listening are this system's limitations.

(e) Other backup communication systems include various means of manual signaling techniques and other signaling methods can be established and implemented at DRO and field activities or local DHA facility through locally developed SOP.

(f) Manual Signal Techniques, Hand, and Arm Signals. These are simple standard or locally devised techniques and procedures used if contact by others means cannot be made or if silence is necessary. The only limiting factor is distance. Regardless of how elaborate other means of communication may be, manual techniques must also be established for guard use.

(g) Weapons: Firing of weapons as a means of communication is used only as a last resort and only in cases of extreme emergency when all other means of communication have failed.

(h) Other means of communication include mass notification systems, sirens, and whistles. Implementation of these devices may be determined locally.

h. The following guidance applies to security guard facilities.

(1) Alarm monitoring facilities should be small-arms hardened (unless underground or located inside of an existing facility). Equipment for alarm monitoring facilities should include landline and LMR capabilities to allow alarm monitors to control entry into structures, shelters, or individual resources in the area and to communicate with on-duty guards. Primary lighting controls for area, boundary, and entry-point lighting should also be included.

(2) ECP or ACP. ECP/ACPs are designed to assist the guard force in controlling entry into and exit from restricted and controlled areas. Guard force planners must ensure ECP and ACPs comply with the following:

(a) Provide landline communication for people requesting entry to the area and direct landline communication to dispatcher.

(b) Protect ECs from the elements by equipping ECPs and ACPs with heating, air-conditioning, light, and ventilation.

(c) Protect ECs from small-arms fire if ECPs or ACPs are not hardened. Hasty fighting positions, barriers, body armor, or other locally constructed items may be used for providing protection.

(3) Security guard armory or arms room - Store guard weapons, ammunition, and equipment in a room or facility that meets the requirements identified in Reference (z).

(4) Alternate Arming Point - DHA sites and facilities should consider establishing an alternate arming point for contingency or emergency purposes. Rooms or facilities used must meet the requirements identified in Reference (z). Guard forces will establish procedures to arm personnel in the event the primary arming point is unavailable (e.g., alternate location, agreement with host DoD installation, hot swapping). Codify these procedures via local instruction.

(5) The Dispatch or Security Control Center is the C2 center for security operations during routine and emergency operations. DHA facility Dispatch or Security Control Center Functions. The Dispatch or Security Control Center serves three C2 functions:

(a) It is the control center to direct guard forces and perform emergency dispatch.

(b) It is the support location for routine operations and command center for the DRO and field activities Director, DO, or SO and AT/Force Protection staff during contingency and expeditionary operations. During contingencies, the Dispatch or Security Control Center manning increases based upon the situation. Additional personnel include persons from the guard staff (Operations) function, as well as other key personnel, as directed by local requirements. Dispatch or Security Control Center equipment can vary based on the DHA facility mission, size, etc.

(c) It is the physical location to achieve command fusion, sensor fusion, and communication fusion for security operations.

(d) As a control center, the Dispatch or Security Control Center may be similar to that of a host DoD installation (e.g., Law Enforcement Desk, Base Defense Operations Center, Emergency Communications Center). Depending upon geographic location (on- or off-installation), security posture, configuration and responsibilities, the DHA facility Dispatch or Security Control Center:

1. Monitors notification, alarm, and alerting systems.

2. Directs and dispatches all assigned guard forces.

3. Documents and records activities.

4. Oversees guard force tactical response and makes notification to key personnel to support the incident commander when required.

5. Up-channels reports as required.

6. Receives public walk-in and telephonic or electronic incident reports.

(e) New Dispatch or Security Control Center facility construction should consider relevant criteria from Reference (al). Where practicable and cost effective, existing facilities should be brought in compliance with UFC standards for new construction. Existing facilities will comply with Reference (d) and this DHA-AI. In the planning stages of new construction or facility upgrade, specific layouts should be determined based upon the size of the unit, mission, etc. Dispatch or Security Control Centers should have a radio system capable of communications with host-installation and off-installation police and fire department(s). Minimum Dispatch or Security Control Center equipment includes:

1. Classified storage (security or law enforcement related purposes only), if necessary.

2. Clocks which show local and Zulu time zones.

3. Installation or DHA site or facility grid maps or computer-based mapping system. Ensure all DHA security guards have and are utilizing the same installation maps or computer-based mapping system the host DoD installation uses.

4. Surveillance camera systems (when used).

5. Radio and telecommunications systems.

6. Duress systems (if applicable unless host-installation response forces are responsible for monitoring IDS for the DHA facility). The DHA facility should coordinate with DHA HQ and host-installation security forces to determine redundant duress requirements for other areas or facilities in conjunction with determining IDS requirements within their supplement. Additionally, the Dispatch or Security Control Center will also contain its own duress activation capability that annunciates at another 24-hour center (e.g., a DHA facility alarm monitoring station or host DoD installation control center).

7. Method of positive entry control and hardened entry door.

8. Interior to exterior intercom.

9. Walk-up window should offer one-way viewing out of the control center.

10. Appropriate weapons racks.

(f) Designate the DHA facility Dispatch or Security Control Center as a controlled area. Access is restricted to personnel authorized access to security, AT, and law enforcement sensitive information.

i. Coordination of forces: Emergency Management response actions of the DHA facility Dispatch or Security Control Center will be consistent with host DoD installation requirements,

designed to incorporate the requirements of Reference (am) and OSD guidance while preserving the unique requirements of the DHA. This provides the DHA with an incident management system consistent with a single, comprehensive approach to incident management. By linking into the host DoD installation emergency management construct, it provides the DHA with the coordinating structures, processes, and protocols required to integrate its specific authorities into the collective framework of Federal departments and agencies for actions to include mitigation, prevention, preparedness, response, and recovery. It includes a core set of concepts, principles, terminology, and technologies covering the incident command system, emergency operation centers, training, ID and management of resources, qualification, and certification, and the collection, tracking, and reporting of incident information and incident resources. The DHA facility Dispatch or Security Control Center provides dispatch and tracking of guard forces during routine and contingency situations. Depending on mission configuration, host-installation agreements, etc., the DHA facility Dispatch or Security Control Center can directly monitor or provide mutual support to host installations by monitoring all emergency reporting and dispatching response elements as required.

(1) Security incident reporting: DRO and field activities Director, DOs, or SOs will follow all information and guidance listed in paragraph 5 of this enclosure, concerning the reporting of suspicious activity and security-related incidents.

(2) FPCON reports: For DHA facilities located on host DoD installations, local Command Posts report FPCON changes (via up-channel reporting) to the respective Service component HHQ. The FPCON alerting process for down-channel messages starts at higher-level HQ and passes down through organizational channels. DHA facility Dispatch or Security Control Centers will report all FPCON changes implemented by the GCC and host or parent DoD installation to the DHA facility Director, DRO and field activities Director, and DHA HQ. GSFs will receive FPCON alert messages via their parent DoD installation or DHA HQ directly.

(3) Force Protection Condition Alerting Message (FPCAM) or down-channel alerting order, sets in motion an increase in readiness posture. As a rule, FPCAMs do not trigger an E-W FPCON change. They give a summary of the situation and offer recommended COAs. DRO and field activities Director, DOs, or SOs then tailor responses to local situations rather than mandating across-the-board actions. Evaluation of reports or current intelligence information may cause an increased state of readiness at a variety of levels. It may affect only one or two DoD installations or DHA sites or facilities, or could possibly affect all DoD installations or DHA sites and facilities E-W. The DHA Operations Center or host DoD installation's Command Post electronically transmits the FPCAM using a military precedence of IMMEDIATE or FLASH. When the FPCAM directs a FPCON change, it is implemented immediately. An FPCON implemented in response to a FPCAM remains in effect until the originating or higher-level authority cancels it. FPCON measures can be found in Reference (an).

(4) Incidents of civil disturbance and requests for disaster assistance or assistance supporting military or civilian law enforcement authorities are handled in accordance with established and approved host-installation emergency response and support plans, and off-installation support agreements with local first responders, as necessary. NOTE: All memorandums of agreement or understanding between host-installation or local first responders concerning requests for assistance

of DHA security guards will first be coordinated through the respective DRO and field activities Director and approved by DHA Chief of Protection Operations.

(5) Reference (ao) prohibits use of DoD personnel for civilian law enforcement purposes except in cases and under circumstances expressly authorized in that instruction *NOTE: Although DHA security guards are not law enforcement officers (e.g., do not have arrest authority), this will also apply to DHA security guards*. This does not prevent the use of security guards to stop a fleeing felon or suspected felon attempting to enter or exit the DHA-controlled site or facility for civilian law enforcement authorities for the purpose of protecting the DHA-controlled site or facility and detaining the individual.

(6) OCONUS procedures - It is the DHA's goal to make every reasonable effort to avoid any confrontation between DHA security guards and host-nation demonstrators or dissidents posing a threat to DHA sites, facilities, personnel, or resources. DHA security guards intervene as specified in host-nation laws, bilateral agreements to which the United States is a party, and international agreements. Local plans to counter such events include provisions to request host-installation, host-nation civil or military support as quickly as possible.

10. FREEDOM OF INFORMATION ACT (FOIA). While administration of the FOIA within DHA is not an element of the physical security program, failure to properly secure or protect information through physical security measures may be subject to requirements under the FOIA regulations, References (ap) and (aq). Additionally, in the case of a breach or unauthorized access, theft, etc., any such documentation can be requested by the public under the FOIA.

ENCLOSURE 4

DHA 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, as defined in Reference (ar). 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. Given the unique and critical mission of DHA facilities, the factors and standards used to determine a Federal FSL have been modified to better address DHA-specific conditions. The five factors quantified to determine a DHAFSL are mission criticality, symbolism, facility population, facility size in square feet (SF), threat to tenant agencies, access to alternate medical care, emergency room, and behavioral health. The FSL determination matrix for DHA facilities is listed in the table below.

Table. The Facility Security Level Determination Matrix

FACILITY SECURITY LEVEL MATRIX – MEDICAL FACILITIES					
	Points				
Factor	Very Low	LOW	MEDIUM	HIGH	
Factor Score	1	2	3	4	Score
Mission Criticality	Negligible or Very Low	Low	Medium	High or Very High	
Symbolism	Negligible or Very Low	Low	Medium	High or Very High	
Facility Population	≤ 100	101 - 250	251 - 750	> 750 or CCC	
Facility Size	≤ 10,000 SF	10,001 – 100,000 SF	100,001 – 250,000 SF	> 250,000 SF	
Threat to Tenants	Low	Medium	High	Very High	
Access to Alternate Medical Care	≤ 20 min	21 – 40 min	41 – 60 min	> 60 min	
Emergency Room Care	Low	Medium	High	Very High	
Neuropsychiatric/Behavior Health Care	Low	Medium	High	Very High	
				Other Factors:	
				Sum of above:	
Facility Security Level:	FSL I Score ≤ 15 pts	FSL II 15-24 pts	FSL III 25-34 pts	FSL IV Score ≥ 35	
Level of Protection (LOP)	Very Low	Low	Medium	High	

3. FSL SCORING CRITERIA. See the DHA security criteria documents for detailed descriptions of each factor. These documents can be found in the Division Documents library at: https://info.health.mil/sites/dos/J3/J34-Home/SitePages/HomePage.aspx

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AA&E	Arms, Ammunition and Explosives
AAR	After Action Report
AC	Access Controller
ACP	Access Control Point
AT	Antiterrorism
ATO	Antiterrorism Officer
BSAT	Biological Select Agents and Toxins
C2	command and control
CAC	common access card
CBRN	Chemical, Biological, Radiological, or Nuclear
COA	course of action
CUI	Controlled Unclassified Information
DCA	Defense Critical Assets
DHA	Defense Health Agency
DHA-AI	Defense Health Agency-Administrative Instruction
DHAR-E	Defense Health Agency-Europe
DHAR-IP	Defense Health Agency-Indo-Pacific
DO	Designated Official
DRO	Direct Reporting Organization
EC	Entry Controller
ECP	Entry Control Point
EPRM	Enterprise Protection Risk Management
ESS	Electronic Security Systems
E-W	enterprise-wide
FDO	Foreign Disclosure Office
FOIA	Freedom of Information Act
FPCAM	Force Protection Condition Alerting Messages
FPCON	Force Protection Condition
FSA	Facility Security Assessment
FSL	Facility Security Level
GCC	Geographic Combatant Commanders
GSA	General Services Administration
GSF	geographically separated facilities
HHQ	Higher Headquarters

HQ	headquarters
ICD	Intelligence Community Directive
ICS	Intelligence Community Standard
ID	identification
IDP	installation defense plan
IDS	Intrusion Detection System
ISC	Interagency Security Committee
ISP	installation security plan
IVA	immediate visual assessment
J-1	Administration and Management
J-3	Operations
J-8	Financial Operations
LMR	Land Mobile Radio
MARMS	Mission Assurance Risk Management System
NIJ	National Institute of Justice
NLW	non-lethal weapon
NVD	night vision device
OCONUS	outside continental United States
PACS	Physical Access Control System
PIV	Personal Identification Verification
PL	protection level
PM	Program Manager
PPBE	Planning, Programming, Budgeting, and Execution
SAPF	Special Access Program Facilities
SCIF	Sensitive Compartmented Information Facilities
SIPRNet	Secret Internet Protocol Router Network
SO	Senior Official
SOP	standard operating procedure
SSO	Small Market and Stand-Alone Medical Treatment Facility Organization
TCA	Task Critical Asset
UFC	Unified Facilities Criteria

PART II. DEFINITIONS

container. Containers used to secure materials and information include safes, cabinets, and vault doors with GSA-approved combination locks or padlocks. Security containers protecting or securing classified areas or material are the responsibility of the Special Security Office.

controlled area. An area that contains resources that require specific security measures to prevent unauthorized entry. Controlled areas are normally assigned to protect DHA assets that directly or indirectly support DHA facilities and the war-fighting mission, and the loss, theft, misuse, compromise, or destruction of which would adversely affect mission capability.

DoD-delegated facility. A DoD-delegated facility is a facility for which DoD has a GSA delegation of authority and occupies space. A DoD nondelegated facility is a facility for which DoD does not have a GSA delegation of authority and occupies space.

Designated Official. For DoD delegated facilities, and at DoD nondelegated facilities where DoD is the largest occupying Federal agency, the senior DoD representative on site will be the Designated Official with FP responsibility for the DoD delegated facility, or the DoD occupants at DoD nondelegated facilities.

ESS. That part of physical security concerned with the safeguarding of personnel and property by use of electronic systems. These systems include, but are not limited to, IDS, automated entry control systems, and video assessment systems.

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 ISC standards.

Market. DHA has administrative sites in the United States that support and report directly to DHA Headquarters. Other DHA sites and facilities in a single geographic area working together with the TRICARE network are aligned into Markets. Each Market is led by a Market office and operates as a system by sharing patients, staff, and budget to improve outcomes, sustain a ready medical force, and create satisfied patients and a fulfilled staff. Director DHA designates a Market Director (generally the most senior DoD health official within the Market) for each Market office. Markets can cross state and national boundaries and should not be conflated with Service areas, regions, districts, etc.

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 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 or activity and the commander or director, must be properly posted, and will employ physical security measures. Additionally, controlled areas may be established adjacent to restricted areas for verification and authentication of personnel.

Senior Agency Official. When the senior DHA official at a facility is not the DO or SO, the DHA official will be appointed the Senior Agency Official to oversee the DHA AT Program only for the DHA-controlled space within the facility.

Senior Official. For DoD nondelegated facilities where DoD is not the largest occupying Federal agency and has not been appointed as DO, the largest DoD occupying tenant's senior representative on site will be the Senior Official, with FP responsibility for DoD occupied tenant areas.

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.