



Defense Health Agency

ADMINISTRATIVE INSTRUCTION

NUMBER 078
September 1, 2022

Director, J-1

SUBJECT: Antiterrorism 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 (p), establishes the Defense Health Agency's (DHA) procedures to:

a. Reissue and cancel Reference (l), to update responsibilities and provide direction for the implementation and establishment of the DHA Antiterrorism (AT) Program and provide guidance on the implementation of References (d) through (f).

b. Deter, detect, delay, deny, defend against, and report on, the full spectrum of terrorist threats directed at DHA personnel, infrastructure, resources, and critical information in order to ensure DHA's continued mission effectiveness.

c. Provide any additional guidance through contacting the DHA Security Branch. The Security Branch central phone number is (703) 681-6777 and SharePoint URL is <https://info.health.mil/cos/admin/ma/Pages/Home.aspx>. The Physical Security Section email box is Dha.physec@mail.mil.

2. APPLICABILITY. This DHA-AI applies to DHA and DHA Activities (under the authority, direction, and control of DHA); all DHA personnel to include: assigned or attached active duty and reserve members, federal civilian employees, contractors (when required by the terms of the applicable contract), and other personnel assigned temporary or permanent duties at DHA; all visitors while within DHA-leased space; and any members of organizations co-located within government-leased spaces in which DHA is the largest organization.

3. POLICY IMPLEMENTATION. It is DHA's policy, pursuant to References (d) and (e), that:

a. DHA has an AT Program in place that meets the requirements set forth in this Instruction, the Interagency Security Committee Standards, the Unified Facility Criteria, as well as

applicable benchmarks and policy as established by the Geographic Combatant Commander (GCC) in whose Area of Responsibility (AOR) a particular DHA site operates. Each DHA site will implement the DHA AT Program and have site-specific information (e.g., local procedures, contingency plans, and operations) addressed in the site's AT Plan (ATP), Emergency Operations Plan (EOP), and/or Occupant Emergency Plan (OEP).

b. In accordance with Reference (f), either a Designated Official (DO), for delegated facilities, or a Senior Official (SO), for non-delegated facilities, will have responsibility for the execution and reporting of the DHA AT Program for DoD occupants, and within the DoD-controlled area of DoD-owned, leased, or managed facilities within the United States Northern Command (USNORTHCOM) AOR. If it is determined that DHA has AT/Physical Security (PS) responsibility for a facility within the USNORTHCOM AOR, whether it is delegated or non-delegated, the highest-ranking DHA employee will assume this responsibility as appropriate. If DHA has not been determined to have responsibility for the execution of the DHA AT Program for the DoD space within the facility as a whole, or the facility is located on a military installation, whether inside or outside the USNORTHCOM AOR, then a Senior Agency Official (SAO) will assume AT responsibility for the DHA-controlled space only.

4. CANCELED DOCUMENTS. This DHA-AI cancels the following document: DHA-AI 078, "Antiterrorism (AT) Program," October 19, 2018.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. PROPONENT AND WAIVERS. The proponent of this publication is the Director, J-1 Administration and Management (A&M). 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. **Not cleared for public release**. This DHA-AI is available to authorized users from the DHA SharePoint site at:
<https://info.health.mil/cos/admin/pubs/SitePages/Home.aspx>.

9. EFFECTIVE DATE. This DHA-AI:

a. Is effective upon signature.

b. Will expire effective 10 years from the date of signature if it has not been reissued or cancelled before this date in accordance with Reference (c).

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

Enclosures:

1. References
 2. Responsibilities
 3. Procedures
- Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....5

ENCLOSURE 2: RESPONSIBILITIES.....6

 DIRECTOR, DEFENSE HEALTH AGENCY6

 DIRECTOR, J-1, ADMINISTRATION AND MANAGEMENT6

 CHIEF, SECURITY BRANCH.....6

 DEFENSE HEALTH AGENCY ANTITERRORISM PROGRAM MANAGER.....7

 DIRECTORS, DIRECT REPORTING ORGANIZATIONS.....9

 FACILITY DIRECTOR, DESIGNATED OFFICIAL, SENIOR OFFICER, DEFENSE
 HEALTH AGENCY SENIOR AGENCY OFFICIAL.....10

 DEFENSE HEALTH AGENCY SITE/FACILITY ANTITERRORISM OFFICER.....11

 ANTITERRORISM REPRESENTATIVE12

 DEFENSE HEALTH AGENCY PERSONNEL12

ENCLOSURE 3: PROCEDURES.....13

 GENERAL PROVISIONS13

 ANTITERRORISM PLAN.....13

 GOVERNANCE OF ANTITERRORISM PROGRAMS15

 INTELLIGENCE16

 ANTITERRORISM OPERATIONS17

 OPERATIONAL REPORTS19

 ANTITERRORISM PROGRAM ELEMENTS19

 RANDOM ANTITERRORISM MEASURES24

 FORCE PROTECTION CONDITION25

 SUSPICIOUS ACTIVITY/INCIDENT REPORTING26

GLOSSARY28

 PART I: ABBREVIATIONS AND ACRONYMS.....28

 PART II: DEFINITIONS.....29

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD (HA))", September 30, 2013, as amended
- (b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013
- (c) DHA-Procedural Instruction 5025.01, "Publication System," August 24, 2018
- (d) DoD Instruction 2000.12, "DoD Antiterrorism Program," March 1, 2012, as amended
- (e) DoD Instruction O-2000.16, Volume 1, "DoD Antiterrorism Standards", November 17, 2016, as amended¹
- (f) United States Northern Command Instruction 10-222, "USNORTHCOM Force Protection Mission and Antiterrorism Program," November 10, 2021²
- (g) Code of Federal Regulations, Title 41, Chapter 101
- (h) United States Code, Title 10, Sections 1072(2) and 1073c
- (i) DoD Antiterrorism Officer Guide, December 2012
- (j) DoD Manual 5200.08 Volume 3, "Physical Security Program," January 2, 2019, as amended
- (k) Joint Publication 3-26, "Joint Combating Terrorism," July 30, 2020³
- (l) Unified Facilities Criteria (UFC) 4-010-01, "DoD Minimum Antiterrorism Standards for Buildings," December 12, 2018, as amended
- (m) Interagency Security Committee Standard, "The Risk Management Process for Federal Facilities," November 2016
- (n) DHA-Procedural Instruction 3700.01, "Director's Critical Information Requirements (DCIR)," Situation Reports of October 4, 2019⁴
- (o) CJCSM 3150.05D, "Joint Reporting System," January 31, 2011
- (p) DoD Instruction O-2000.16-V2, November 17, 2016 Change 1, May 8, 2017
- (q) DoD Instruction 4000.19, "Support Agreements," December 16, 2020
- (r) DHA-Administrative Instruction 097, "Insider Threat Program," September 6, 2018

¹ This reference is available at: This document is available on the DOD Issuances Website <http://www.esd.whs.mil/Portals/54/Documents/DD> and is only available to those with Common Access Card authorization.

² This reference is available at: <https://portal.noradnorthcom.mil/library/pubs/sitepages/home.aspx>

³ This reference is available at: <https://jdeis.js.mil/jdeis/index.jsp?pindex=2>

⁴ This reference is available at: <https://info.health.mil/cos/admin/pubs/DHA%20Administrative%20Instructions%20Signed/Forms/AllItems.aspx>

ENCLOSURE 2
RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA, will:
 - a. Assume overarching responsibility for the DHA Antiterrorism (AT) Program.
 - b. Designate the Security Branch as office of primary responsibility for managing and executing the DHA AT Program enterprise-wide (E-W).

2. DIRECTOR, J-1 (A&M). The Director, J-1 (A&M) will:
 - a. Provide executive-level oversight, direction, and support to the Office of Primary Responsibility, in the execution of the tasks and responsibilities indicated below.
 - b. Coordinate with the DHA Financial Operations Division to program funds in accordance with the DHA Program Objective Memorandum cycle to reduce vulnerabilities and mitigate risks to DHA assets, through procedural (e.g., policy, guidance, organization) or physical (e.g., vehicle barriers, perimeter fencing, electronic security systems) measures.
 - c. Ensure the appropriate executive-level civilian or military officer (i.e., Direct Reporting Organization (DRO) Director, DO, SO, or SAO) attends AT Level III training for Commanders and Directors in accordance with Reference (e).

3. CHIEF, SECURITY BRANCH. The Chief, Security Branch will:
 - a. Direct the coordination of the DHA AT Program with other security disciplines organic to, or in support of DHA, such as personnel security, operations security, information security, counterintelligence, and the insider threat program, in order to provide an integrated and coherent overall security effort. DHA policies for other security disciplines are posted at: <https://info.health.mil/cos/admin/pubs/DHA%20Administrative%20Instructions%20Signed/Forms/AllItems.aspx> .
 - b. Serve as approval authority for AT guidance/policy and waiver authority for requirements in this publication.
 - c. Execute the strategic AT planning functions.
 - d. Develop and maintain a single source document that states the common DHA security mission and vision. Additionally, through a strategy-to-task process, provide authoritative guidance concerning all security-related activities.

- e. Provide a broad perspective on AT policy reviews, including the review of policy documentation and providing recommended changes to support developing concepts and doctrine.
- f. Provide DHA advocacy for the acquisition, sustainment, and research and development in support of all physical security systems acquired to meet DoD AT policy requirements. Approve the acquisition of any physical security system and equipment E-W in support of the DHA AT Program.
- g. Provide strategic direction, policy, and planning guidance for DRO security and contingency planning, in accordance with governing DoD and DHA guidance.
- h. Perform DHA E-W security Planning, Programming, Budgeting, and Execution (PPBE) that considers the impact of risk for DHA sites, facilities, and other locations where DHA is the lead organization with AT responsibility.
- i. Allocate, distribute, and oversee the execution of AT funding in support of DRO and Combat Support requirements.
- j. Manage the DHA Risk-Management program.
- k. Perform Capacity Building Operations. Capacity Building, also known as Building Partnership Capacity, will require close communication with DRO staffs. This includes:
 - (1) Identifying mission partner capability gaps in supporting DROs and contingency plans. Develop courses of action (COAs) to mitigate capability gaps.
 - (2) Liaising with Military Departments, DoD Components, and federal agency partners and providing training and mentorship to develop AT capacity.
 - (3) Providing training venues and opportunities to partner with security personnel in the DHA enterprise.
- l. Establish a DHA Mission Assurance Assessment Team in accordance with DoD guidance, to facilitate Headquarters (HQ)-level AT Program reviews, assessments, and inspections. Develop E-W a triennial assessment and inspection schedule.

4. DHA AT PROGRAM MANAGER. The DHA AT Program Manager is the Senior AT Advisor to the Chief, Security Branch. The DHA AT Program Manager will ensure E-W compliance and uniform execution of the AT Program to include:

- a. Coordinate with DHA Physical Security Program Manager to consolidate E-W PPBE funding and acquisition requests regarding physical security equipment and services and submit to the Chief, Security Branch in support of the DHA AT Program.

- b. Develop policy and procedures for conducting investigations concerning threats and terrorism related incidents. Monitor the conduct of such investigations by civilian, host nation, DoD, or other law enforcement agencies. Provide applicable results of terrorist-related investigations to the Chief, Security Branch.
- c. Provide support for the Chief, Security Branch mission to source DHA AT Program requirements.
- d. Provide guidance to DHA Mission Assurance Assessment Team in accordance with DoD and DHA requirements, concerning AT Program reviews, assessments, and inspections.
- e. Coordinate with the DHA Physical Security Program Manager, as needed, concerning the DHA Security Waiver Control program. Assist the DHA Physical Security Program Manager with reviewing and providing feedback on waiver requests, in close coordination with the DRO.
- f. Develop and maintain the DHA AT Program Administrative Instruction, to include other documents (e.g., Procedural Instructions, Handbooks) as required.
- g. Provide AT subject matter expertise and recommend policy changes to the Chief, Security Branch, supporting the development of future AT concepts, guidance, and program management.
- h. Provide state-of-the-art training, tools, and products, including but not limited to Mission Assurance Risk Management System (MARMS) and Enterprise Protection Risk Management (EPRM) for the DHA community. Oversee the DHA E-W Risk-Management program, to include the use, permissions, and administration of EPRM and MARMS.
- i. Provide guidance and training expertise as part of the Lessons Learned process.
- j. Manage current and future AT Program requirements based on program deficiencies and coordinate with DHA Physical Security Program Manager concerning the development and review of new technology and procedures.
- k. Represent the Chief, Security Branch, concerning the DHA AT Program in HQ-level conferences and committees.
- l. Assist the DHA Physical Security Program Manager with reviewing all Facility Security Assessment results involving DHA-leased space, as well as DROs, to include the proposed Facility Security Level.
- m. Coordinate with the DHA Emergency Management Program as appropriate, to assist with plan development, event reporting, risk assessment (RA), and response tactics, techniques, and procedures to ensure each program effectively supports the other at HQ, DRO, and facility levels.
- n. Coordinate and work closely with DRO Directors on program management.

(1) Coordinate across DHA to plan and program for DROs and Combat Support requirements directly impacting risk management.

(2) Review and approve or disapprove all security waiver requests, as requested by DRO and Facility Directors.

5. DIRECTORS, DIRECT REPORTING ORGANIZATIONS. The DRO Directors are responsible for management, compliance, and uniform execution of the AT Program for all assigned facilities, and will appoint an organization AT Officer (ATO) in writing.

6. ORGANIZATION ATO. The organization ATO will provide direct execution support to their assigned facilities, as well as provide support to the host or parent installation (closest DoD installation providing AT support) and respective GCC, as appropriate. Specifically, the organization ATO will:

- a. Define requirements for facility AT operations.
- b. Prioritize facility AT requirements.
- c. Serve as senior AT advisor to the DRO Director.
- d. Manage and guide the AT program within their respective organization.
- e. Ensure the EPRM and MARMS asset rankings are consistent throughout the facilities during visits and routine operational correspondence.
- f. Oversee the DHA Risk-Management program, to include the use of EPRM and MARMS for their assigned facilities and coordinate closely with host or parent installations (if needed) to:
 - (1) Identify, plan, and program for AT requirements directly impacting risk management.
 - (2) Ensure facilities document and submit security waiver requests to DRO Director for coordination and review, prior to submitting to Chief, Security Branch.
- g. Develop organization-specific AT requirements for unique systems, resources, and facilities via supplement to this Instruction as needed.
- h. Coordinate with the DHA AT Program Manager to schedule AT Program reviews, assessments, and inspections.
- i. Direct validation of manpower and resource allocation in support of the AT Program.
- j. Ensure DHA facilities are executing their ATP and following DoD and GCC guidance.

k. Consolidate AT Programs and processes PPBE funding and acquisition requests from all assigned facilities, for submission to the DHA AT Program Manager.

l. Review all personnel contracts and all other contracts above the \$150K threshold to ensure they satisfy antiterrorism requirements. Complete reviews within three working days of receipt, during the contract development stage prior to the local or DHA contracting office review. The ATO may combine this with the Operations Security review if the ATO is level II certified in both programs.

6. FACILITY DIRECTOR, DO, SO, DHA SAO. The Facility Director, DO, SO, or SAO is responsible for the execution of the AT Program within their assigned facilities. The Facility Director, DO, SO, or SAO will:

a. Ensure an OEP and EOP are developed, implemented, and maintained for their assigned facilities in accordance with Reference (m). Distribute the OEP and EOP to all facility occupants.

b. Coordinate with their respective DRO ATO (or DHA AT Program Manager when there is no DRO ATO) to clarify any issues concerning the execution of the AT Program within their assigned facilities.

c. Develop and maintain a comprehensive ATP in accordance with Reference (e). NOTE: DHA tenants on DoD installations will partner and liaise with the responsible installation security/law enforcement AT offices to coordinate on any local or specific needs not addressed in this DHA-AI.

d. Develop and implement site-specific Force Protection Condition (FPCON) Action Sets in accordance with Reference (e).

e. Ensure all required AT program assessments (e.g., criticality, threat, and vulnerability) are conducted via EPRM, in accordance with Reference (d).

f. Identify and consolidate site-specific funding and acquisition requests regarding AT program equipment and services for submission to DRO Director.

g. Execute DHA Risk-Management program for their respective facilities and coordinate closely with DRO Directors and host or parent installations (if needed) to:

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

(2) Document and submit security deficiencies and waiver requests to the DRO Director for coordination and review prior to submitting to Chief, Security Branch.

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

h. Establish and develop local AT programs for DHA standalone, geographically separated facilities (GSF), dispersed sites and other like facilities not located on a DoD installation, or for those DHA sites or facilities located on a host or parent installation, provide all required information to their host or parent installation for inclusion in the installation ATP, defense plan, or similar document. The host or parent installation will provide administrative support and guidance for conducting the EPRM at these locations. The Facility Director, DO, or SO will present the EPRM results and potential COAs to the responsible installation commander's Integrated Defense Council or other responsible council/committee, in order to make risk management decisions. The Facility Director, DO, or SO is responsible for documenting approved COAs in the host or parent installation's ATP and similar documents, and ensuring appropriate support agreements are in place and sufficiently address AT needs at the location.

(1) GSFs will 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 or the GCC, and consistent with DHA directives and local memorandum of understanding, support may include security guard participation to secure mission assets in their immediate work areas, sites, facilities, compounds, etc.

(2) GSFs will ensure asset criticality is considered during the development and review of a support agreement. The host or parent installation will execute COAs to create desired AT effects to mitigate risk to the assets in accordance with the installation commander's or GCC's and Facility Director's risk tolerance decision.

(3) Facilities with existing support agreements will ensure DHA personnel, assets and associated COAs are included within the host or parent installation's EPRM process, contained in the installation's defense and security plans, and are reviewed annually.

i. Ensure all assigned DCA/TCA/Tiered Assets and other protection level resources, security waivers, vulnerabilities, compensatory measures, planned projects, etc., are documented via MARMS.

j. Ensure Random AT Measures (RAM) are conducted in accordance with Reference (e).

7. DHA SITE/FACILITY ATO. Each DHA site and facility tasked with AT/Force Protection (AT/FP) responsibility will have an ATO assigned, in writing, by the respective Director, DO, SO, or SAO. The ATO will:

a. Implement and oversee the AT program, on behalf of the Director, DO, SO, or SAO for the site(s) to which they have been appointed.

- b. Develop and maintain the ATP and related documents (e.g., procedural instructions, handbooks, as needed), and review each document annually.
 - c. Coordinate with DHA and host or parent installation to identify specific actions and measures to be implemented for each FPCON.
 - d. Facilitate all AT program assessments (e.g., criticality, threat, and vulnerability), ensuring all are accomplished via EPRM, in accordance with Reference (d).
 - e. Complete a formal, Level II ATO training course of instruction, whether a course in residence or through a Mobile Training Team in accordance with Reference (i). Newly appointed ATOs, or ATOs who have not served as such in the past three years, must complete this training.
 - f. Attend refresher training every three years by attending a DoD-sponsored AT conference, or a Level II ATO training course through in-residence, Mobile Training Team, or web-based distance learning instruction. ATOs who have served as such on a continual basis must also attend refresher training in-residence.
 - g. Verify and document all DHA personnel complete initial and annual AT Level I training in accordance with in accordance with References (e) and (i).
 - h. Monitor and track the implementation and completion of Random Antiterrorism Measure for all assigned sites or facilities.
8. AT REPRESENTATIVE (ATR). A DHA DO or SO may choose to appoint, in writing, a civilian employee, military, or DoD contractor ATR (pursuant to an applicable contract) to assist in the execution and daily functioning of the DHA AT Program within their assigned facilities. In addition to daily functions, the ATR will:
- a. Complete a DoD-approved, Level II ATO training course.
 - b. Liaise with and support their respective ATO regarding all elements of the local AT Program.
9. DHA PERSONNEL. All DHA personnel will complete annual AT Level I awareness training in accordance with Reference (e).

ENCLOSURE 3

PROCEDURES

1. GENERAL PROVISIONS. The implementation of the AT Program at each DHA site will meet the requirements put forth in this DHA-AI, as well as applicable regulations and assessment benchmarks. If a particular requirement is considered unattainable, enter a justification and mitigation plan in MARMS for review by GCC. All DHA ATPs, EOPs, and OEPs must be approved by the individual responsible for the execution of the plans within their assigned facilities. If DHA does not have AT/FP responsibility for the facility, then the SAO will develop an annex to the established site ATP.

2. AT PLAN

a. The purpose of the AT Plan, in accordance with Reference (e), is to provide organization-specific guidance and execution oriented instructions for subordinates; assign roles, missions, and functions; and identify resources Facility Directors, DO, or SO require to enable them to remediate or mitigate the risks from terrorist threats. The ATP is designed to provide specific instructions, assign responsibility, and coordinate support for emergencies or situations involving potential or actual terrorism-related events. ATPs direct the implementation of DoD AT standards and must be tailored to the level of the organization.

b. For all on-installation DHA tenants responsible for FP, the host or parent installation will have an ATP that should include all tenants, resources, personnel, etc. As a mission partner (tenant), Facility Directors, DO, or SO will:

- (1) Review the host or parent installation ATP.
- (2) Identify and understand all agency responsibilities.
- (3) Ensure the plan addresses the specific needs of DHA sites/facilities.
- (4) Identify any mission impacts and concerns, and address them accordingly.

(5) Ensure their site/facility ATP complements the host or parent installation's ATP, and provide host or parent installation with a copy.

c. For DHA tenants in shared sites/facilities, where the DO, or SO is not responsible for FP, they will:

(1) Review the site/facility ATP. NOTE: In accordance with Reference (f), the primary (largest) tenant has overall FP responsibility and is required to have an ATP established that includes all site/facility tenants.

(2) Identify and understand all agency responsibilities.

(3) Ensure the plan includes and addresses any specific DHA support requirements.

d. At GSFs, to include those sites/facilities where DHA has been tasked with overall FP responsibilities, Facility Directors, DO, or SO will develop an ATP in accordance with Reference (e) AT Standard 7 and this instruction. Facility Directors, DO, or SO will:

(1) Coordinate with their host or parent installation AT office concerning the development and coordination of the site/facility ATP.

(2) Identify, coordinate, and codify any specific support requirements via installation support plan, memorandum of agreement, etc.

(3) For GSA-leased facilities or spaces that have more than one federal (non-DHA) tenant, DO or SO tasked with FP responsibility will ensure the plan includes these other agencies by coordinating with them via Facility Security Committee. Site/facility DO or SO should follow all Interagency Security Committee guidance concerning Facility Security Committee.

e. Elements of the ATP must include: intelligence, personnel, operations, exercises and training, resource application, and coordination. Facility Directors, DO, or SO will approve and sign ATPs, giving the plan(s) authority equivalent to military orders. To provide additional support to AT operations as appropriate to the threats in their assigned facilities, Facility Directors, DOs, or SOs ensure that their ATPs also address the following subjects:

(1) Command and control for overall AT plan execution.

(2) Task organization of AT organizations and capabilities.

(3) AT concept of operations to employ protection capabilities and achieve the Facility Director, DO, or SO intended outcomes.

(4) Logistics and contracting requirements.

(5) Specific risk-mitigation measures that serve to establish the baseline defensive posture.

(6) Transitioning to and from elevated security postures, including FPCON measures and FPCON levels.

(7) Chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) response operational fundamentals of prepare, prevent, protect, respond, and recover.

(8) CBRNE response consequence management fundamentals.

(9) Counter weapons of mass destruction (WMD) fundamentals.

(10) Access control measures.

(11) Mass warning and notification systems and recall procedures.

f. ATPs containing information linking a site with the risk-mitigation measures employed at the site and an FPCON level are considered controlled unclassified information at a minimum. Commanders will ensure that controlled unclassified information is marked, safeguarded, and disseminated appropriately.

g. Facility Directors, DO, or SO will establish procedures to review their ATPs for classified information and place any necessary classified information in classified annexes. Safeguard and appropriately mark ATPs that contain classified information.

h. Facility Directors, DO, or SO will ensure their ATPs receive a DHA legal review when appropriate for their mission from their servicing DHA Office of General Counsel attorney.
NOTE: Recommend DHA tenants coordinate with both DHA and host or parent installation legal offices.

3. GOVERNANCE OF AT PROGRAMS. DHA has sites/facilities located both on and off DoD installations throughout the world. Because of this, meeting this DoD requirement presents various challenges. Include or reference charters for the following AT governance groups, or other groups that execute the functions which are the responsibility of the host or parent installation that is responsible for AT/FP, in the facility ATP.

a. AT Working Group (ATWG). ATWGs are normally chaired by the installation commander (or civilian equivalent) responsible for AT/FP. The ATWG is required to meet at least semi-annually, or more frequently depending on the level of threat, to oversee the implementation of the AT Program, to develop and refine ATPs, and to address emergent or emergency AT issues. ATWG membership is determined by the installation commander, and will normally include the installation ATO, senior staff representatives, senior representatives from DoD tenant organizations, and other representatives as required (including Pentagon Force Protection Agency (PFPA) and Federal Protective Services (FPS) in the National Capital Region) to support AT planning and program implementation.

(1) The DRO Director and ATO may attend the host or parent installation ATWG on behalf of all assigned DHA sites/facilities. Individual Facility Directors, DO, or SO may be invited to attend installation ATWGs on an as needed basis.

(2) The DRO ATO will be responsible for obtaining and distributing copies of the host or parent installation ATWG meeting minutes.

b. AT Executive Committee (ATEC). ATECs are normally chaired by the installation commander responsible for AT/FP. The ATEC meets at least semi-annually to develop and refine AT program guidance, policy, and standards in order to act upon recommendations of the

ATWG and the Threat Working Group, and to determine resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities. ATEC membership is determined by the installation commander, and will normally include the installation ATO, senior staff representatives, senior representatives from DoD tenant organizations, local, State, Federal, and host-nation security and law enforcement organizations (such as PFPA and FPS), and other representatives as required to support AT planning and program implementation.

(1) The DRO Director and ATO may attend the host or parent installation ATEC on behalf of all DHA sites/facilities within the assigned DHA sites/facilities. Individual Facility Directors, DO, or SO may be invited to attend installation ATECs on an as needed basis.

(2) The DRO ATO will be responsible for obtaining and distributing copies of the host or parent installation ATEC meeting minutes.

c. Threat Working Group (TWG). TWGs are normally chaired by the installation commander responsible for AT/FP. The TWG will meet at least quarterly to develop and refine terrorism threat assessments (TA); and coordinate and disseminate threat warnings, reports, and summaries. TWG membership is determined by the installation commander, and will normally include the installation ATO, senior staff representatives, senior representatives from DoD tenant organizations, local, State, Federal, and host-nation security and law enforcement agencies (such as PFPA and FPS), and other representatives as required to support AT planning and program implementation.

(1) The DRO Director and ATO may attend the host or parent installation TWG on behalf of all assigned DHA sites/facilities. Individual Facility Directors, DO, or SO may be invited to attend installation TWGs on an as needed basis.

(2) The DRO ATO will be responsible for obtaining and distributing copies of the host or parent installation TWG meeting minutes.

4. INTELLIGENCE

a. Intelligence gathering, fusion, and threat analysis is a challenging effort for DHA, as it has sites/facilities located both on and off DoD installations throughout the world. Because of this, there is no one, specific organization tasked with facilitating coordination of threat information, to include analytical efforts focused on identifying current and emerging actors posing a threat to DHA interests. Most, if not all, DHA sites/facilities located on host or parent installations receive intelligence/threat information from the ATWG and TWG. Other DHA sites/facilities, receive information directly from Combatant Commands and components (e.g., USNORTHCOM, U.S. Army Forces Northern Command, U.S. Air Forces Northern Command).

b. For DHA tenants of host or parent installations, Facility Directors, DO, SO, or SAO, will coordinate with host or parent installation ATO office for all intelligence/threat information.

c. For GSFs, DO, or SO will coordinate with their host or parent installation AT office, local, State, Federal, and host-nation security and law enforcement organizations (such as PFPA and FPS), and other agencies as needed. NOTE: FPS does not provide specific AT program support but can assist with coordinating and identifying threat/crime information.

d. The DHA Foreign Travel Office will provide travel briefs and debriefs to personnel traveling outside of the United States or its associated territories. Specific guidance will be given pertaining to threats, activities, and AOR requirements in accordance with the Foreign Travel Clearance Guide.

5. AT OPERATIONS. AT operations are based on a layered defense, underpinned by FP measures, security, and law enforcement services. Electronic and physical layered defenses may include the following: access control systems and measures, closed circuit television systems, FPCONs, RAMs, law enforcement patrols, and surveillance detection teams. Inner layers of defense include roving patrols, office access controls, defined security zones, and physical security measures. Enforcement of Interagency Security Committee/Unified Facility Criteria Standards will support layered defenses. Facility Directors, DO, and SO will execute AT operations via the following phases:

a. Pre-incident Phase. Pre-incident Phase consists of the execution of baseline AT measures emphasizing preventive and deterrent measures; physical security and law enforcement; training and exercising; establishment of memorandums of agreement (MOA) in accordance with Reference (q); development of plans to protect High Risk Personnel; intelligence/threat analysis; and the execution of security measures within DHA sites/facilities. Planning efforts should include coordination with the host or parent installation, AT/FP working groups, and other appropriate agencies.

(1) Baseline AT measures include:

(a) Category 1, Administrative includes, but is not limited to, establishing an AT Program, conducting AT Level I Awareness Training, the identification (ID) of High Risk Personnel, and drafting and validating AT contingency and emergency plans.

(b) Category 2, Physical Security includes, but is not limited to, access control (may include security guards, badging, electronic access systems, magnetometers, X-ray, and visitor screening and control), mass notification systems, emergency notification systems, mail distribution procedures, parking control, construction standards, and camera systems.

(c) Category 3, Special Purpose Enhancements include, but are not limited to, hostile surveillance operations and mitigations for CBRNE and WMD.

(2) Required pre-incident supporting tasks and products include, but are not limited to:

(a) Annual TAs and periodic updates.

- (b) Criticality and VAs.
- (c) Risk analysis.
- (d) Development of curtailment actions and AT/physical security measures.
- (e) Training and exercises.
- (f) Terrorist Incident Responses.
- (g) Terrorist consequence management, to include increase in FPCON measures, evaluation of the Continuity of Operations Plan/business continuity plan, and implementation of a Crisis Action Team.
- (h) Annual ATP reviews.
- (i) AT resource requirement ID, documentation, and submission.
- (j) Execution of FPCON measures and RAMs.

b. Incident Phase. In the event of a terrorist attack affecting DHA locations, initiate and coordinate terrorist incident response procedures through the rapid establishment of an Emergency Command Center and a Crisis Action Team. NOTE: Host DoD installations are responsible for accomplishing this task. Terrorist incident response measures will address the full scope of DHA and local jurisdiction response capabilities. Dependent on the scope of the emergency and the location, initiate site-specific ATP and/or Continuity of Operations Plan.

(1) Local law enforcement or security guards will respond to incidents occurring at or near DHA sites. NOTE: For DHA tenants on DoD installations, the host or parent installation is the lead law enforcement/investigative agency that will provide direction to supporting agencies and determine when to transition to consequence management operations. For GSFs, specific guidance and direction will be determined via support plans, MOAs, etc.

- (b) This phase includes:
 - 1. Crisis Response.
 - 2. Serious Incident Reporting.
 - 3. Recovery of casualties and treatment of the injured.
 - 4. Containment of the incident.
 - 5. Abatement of life-threatening hazards.
 - 6. Evacuation of potentially threatened areas.

c. Post-incident Phase. Host or parent installation and local emergency responders will assist in synchronizing recovery efforts. All evidence and forensic information found during post-incident investigation will be collected, handled, and kept by the primary law enforcement/investigative agency. This phase ends when the local jurisdictions, DHA site(s), and the surrounding community have stabilized, and normal mission requirements can resume. Restoration of normal operations includes:

- (1) Restoration of primary, alternate, and tertiary evacuation routes.
- (2) Restoration of support and utility services.
- (3) Debris and hazardous material cleanup and disposal.
- (4) Resettlement of displaced personnel.
- (5) Situation reports and follow-up investigations.
- (6) Stand-down of crisis management personnel.

6. OPERATIONAL REPORTS (OPREP). For DHA sites/facilities located on DoD installations, the host or parent installation law enforcement will respond, conduct any/all investigations, and up-channel the reports through the respective installation Command Post in accordance with the appropriate Situation Report or OPREP category and procedures specified by Reference (o), Situational Monitoring Manual, or otherwise directed local procedure. Facility Directors, DO, or SO should identify, coordinate, and establish any additional support or notification requirements via installation support plan, MOA, etc.

7. AT PROGRAM ELEMENTS. AT Program Elements include AT risk management, planning, training and exercises, resource application, and program reviews. The development of these elements should be ongoing to ensure the viability of all defensive measures employed to reduce DHA's vulnerability to terrorist attacks.

a. AT RA. Components of the AT Risk Management process include assessing the threat (the terrorism TA), identifying the assets most important to protect (the criticality assessment (CA)), and determining which of those important assets are most vulnerable (the vulnerability assessment (VA)), as listed in References (e) and (k).

b. Accomplishing AT RAs. All AT RAs will be accomplished by utilizing the EPRM. NOTE: Each facility ATO or designated security representative must have access to EPRM/MARMS, via Secret Internet Protocol Router Network, to review and complete all tabs (DoD MA Assessment Elements).

(1) TA. Terrorist TAs will be reviewed annually for each DHA site/facility and integrated into the Risk Management process. Event-specific TAs may be requested to support

operational planning and risk decisions for special mission requirements including, but not limited to, training and exercises, operational deployments, and special events.

(a) For DHA tenants of host or parent installations, the local TA is generally provided by the lead Military Department investigative agency (e.g., Air Force Office of Special Investigations, Army Criminal Investigation Command, Naval Criminal Investigative Service). Facility Directors, DO, or SO, will coordinate with host or parent installation ATO office for this information.

(b) For GSFs, Directors, DO, or SO will coordinate with their host or parent installation ATO Office, local, State, Federal, and host-nation security and law enforcement organizations (such as PFPA and FPS), and other applicable agencies as needed. NOTE: FPS does not provide specific AT program support but can assist with coordinating and identifying threat/crime information.

(2) CA. Critical assets are any facility, equipment, service, or resource considered essential to DoD operations in peace, crisis, and war. Critical assets can be people, property, equipment, activities and operations, information, facilities, or materials. Critical assets warrant measures to protect from disruption, degradation, and destruction, and to ensure continued operation. Facility Directors, DO, or SO, in coordination with their ATO, will develop a prioritized, mission essential asset (DCA, TCA, Tiered Assets, and Protection Level Resources) listing for each DHA site/facility.

(a) In accordance with Reference (e) AT Standard 5, Facility Directors, DO, or SO will conduct and review CAs at least annually and update them based upon asset importance, effect of loss, recoverability, mission functionality, substitutability, and reparability.

(b) Facility Directors, DO, or SO will identify and evaluate an organization's assets based on the importance of their mission or function, the group of people at risk, and the significance of a facility.

(3) VA. The VA is used to determine the susceptibility of assets to attack from threats identified in the TA. VAs are required to be conducted, updated, and recorded annually, at a minimum, for all DHA sites/facilities in accordance with Reference (e). VAs will incorporate the DoD Mission Assurance Assessment benchmarks and be consistent with the principles outlined in Reference (j) and local AT guidance.

(a) For DHA tenants of host or parent installations, the local VA is generally conducted by the installation AT office. Facility Directors, DO, or SO, will coordinate with host or parent installation ATO to obtain identified vulnerability information for input into EPRM.

(b) For GSFs, Directors, DO, or SO will coordinate with their host or parent installation AT office, local, State, Federal, and host-nation security and law enforcement organizations (such as PFPA and FPS), and other applicable agencies as needed, in order to obtain identified vulnerability information for input into EPRM. NOTE: FPS does not provide

specific AT program support but can assist with coordinating and identifying threat/crime information.

(4) Risk Analysis. The risk analysis combines the results of the CA, TA, and VA to facilitate informed risk evaluations, decisions, and responses. The risk analysis is the final step in the overall assessment process.

(a) For DHA tenants of host or parent installations, Facility Directors, DO, or SO will develop, in coordination with the host or parent installation, courses of action to accept, remediate, or mitigate risk. Facility Directors, DO, or SO, will ensure all courses of action are recorded in MARMS.

(b) For GSFs, Directors, DO, or SO will develop, in coordination with their host or parent installation AT office, local, State, Federal, and host-nation security and law enforcement organizations (such as PFPA and FPS), and other applicable agencies as needed, courses of action to accept, remediate, or mitigate risk. Facility Directors, DO, or SO, will ensure all courses of action are recorded in MARMS.

(c) Resource Application. Where procedural or existing structural measures are insufficient for reducing vulnerabilities or mitigating risk, funds for mitigation measures may be requested from the DHA Financial Operations Division. Requested changes, improvements, and construction projects will be coordinated through the respective DRO Office with the assistance of the host or parent installation, General Services Administration (GSA), and DHA Security Branch, as necessary.

1. MARMS provides the principal mechanism for prioritizing AT resource requirements and responsibilities for input into the DHA PPBE process or Combatant Commander Initiative Fund.

2 Chief, Security Branch, will coordinate through the Director, J-1 (A&M) for approval of all Combatant Commander Initiative Fund submissions and requests for funding through the PPBE process, and will advocate for resources for unfunded requirements affecting the AT Program or overall FP mission.

c. Training and Exercises.

(1) AT Operations. Facility Directors, DOs, and SOs have broad flexibility to adapt AT operations for local conditions. AT operations will vary widely between locations. These variances create unique challenges in verifying accountability and validating operational proficiency/readiness.

(2) AT/Response Force Training. Security guards should coordinate planning, tactics, and rehearsals with host or parent installation and local law enforcement (if partnered with via support agreement). Effective, realistic training through “force-on-force” exercises is manpower and resource intensive, and often facility security guards are limited by local conditions from conducting all “mission-specific” training they most need. Computer-based training/simulator

systems provide realistic training tools to supplement (rather than replace) live training and their use is highly encouraged. Facility Directors, DO, or SO should make every effort to ensure those tasked with providing security response are familiar with and competent in with security tactics, techniques, and procedures.

(3) AT Level I Training. All DHA personnel and contractors are required to complete AT Level I training annually. Web-based AT Level I training is available at the Joint Knowledge Online (JKO) website: <https://jkodirect.jten.mil/>. NOTE: Assigned military personnel will follow their respective Military Department requirements for completing AT Level I training. Facility Directors, DO, or SO are responsible for ensuring all training is accomplished for their assigned personnel.

(a) The ATO or ATR (collectively abbreviated ATO/R) will monitor and track AT Level I training completion via JKO. Requests for “reports manager” access in JKO should be coordinated through the DHA Learning & Development Division.

(b) The ATO/R will provide quarterly training completion and deficiency statistics in January, April, July, and October to the Facility Director, DO, or SO and be prepared to provide this information to others upon request (e.g., DRO Director, DHA HQ Assessment Teams).

(4) AT Exercises. AT exercises allow the DHA sites/facilities, as well as supporting forces the ability to simulate FPCON and contingency actions they could not otherwise effectively practice during daily operations. Facility Directors, DO, or SO will work closely with the host or parent installation emergency responders to conduct joint-AT training exercises. GSFs will coordinate and work closely with their host or parent installation, local, State, Federal, and host-nation security, law enforcement organizations (such as PFPA and FPS), and local emergency services personnel to conduct AT exercises. 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.

(a) Local Exercises. Conduct local exercises as frequently as needed to maintain a high degree of readiness.

1 Multiple attacks in recent years have employed fire as a weapon. Small arms have also been used in numerous attacks on military facilities. Therefore, the annual AT exercise schedule will incorporate at least one evacuation for fire and one active shooter. Design exercises so they will not impede mission essential activities or create hazards to health, life, and safety.

2 Exercise at least one hostile threat scenario involving all facility security and response forces annually. Coordinate and conduct all proposed exercises in conjunction with other required and scheduled exercises. Coordination and planning with host or parent installation, FPS, and local emergency services is crucial to the development and execution of relevant exercise scenarios (e.g., increased FPCONs, mass casualty, AT, or CBRNE attack).

(b) Contingency Exercise Requirements. DRO Directors, host or parent installation(s) and local facilities identify the types of contingency actions that will be exercised.

(c) Host or Parent Installation Exercises. Facility Directors, DO, or SO will coordinate with host or parent installation to develop specific training and annual exercise schedules. Exercises should test the AT plan against identified threat capability. Conduct exercises in accordance with locally established exercise, evaluation, and safety guidance. Facility Directors, DO, or SO will make every effort to ensure maximum participation in exercises. NOTE: Design scenarios to test effectiveness of countermeasures against threats that target known vulnerabilities where risk has been accepted. If the exercise provides compelling indicators that the risk acceptance is inappropriate, the ATO/R will present this issue to the Facility Director, DO, or SO and request revised guidance. This additional guidance should be documented (e.g., update AT plan, EPRM, MARMS) and the planning process should be repeated.

1. Annual Exercises. For annual exercises, members of the exercise evaluation team, in coordination with the host or parent installation, should develop scenarios utilizing adversarial 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 COAs.

2. Exercise Evaluation/After Action Review (AAR). Facility Directors, DO, or SO will ensure an exercise evaluation is conducted and documented via AAR. NOTE: If the host or parent installation is responsible for the AAR, Facility Directors, DO, or SO will request and maintain a copy on file.

(d) Staff Assistance Visits. DHA HQ and each DRO should develop visit programs to meet their intent and needs as a Higher Headquarters (HHQ) or as requested by the facility (e.g., inspection preparation, program review). Use these visits to identify and resolve problems and allow responsible installation agencies to join in planning and programming actions.

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

(5) AT Program Reviews (ATPRs). ATPRs evaluate the effectiveness and adequacy of AT program implementation and assess compliance with AT Standards. Local ATPRs will be conducted annually in conjunction with the site VA and triennially as a DHA Higher Headquarters Assessment. The Office of Primary Responsibility will promulgate an annual DHA Higher Headquarters Assessment schedule indicating sites to be assessed each January through March, April through June, July through September, and October through November. An ATPR must also be conducted whenever significant changes in threat, vulnerabilities, or asset criticality occur. External ATPRs may be coordinated through the nearest military or DoD security forces command or installation.

(a) An annual review or update via MARMS of all information will be conducted by the ATO or designated security representative on behalf of the Facility Director, DO, or SO. DHA tenants or GSFs will coordinate with the host or parent installation, if necessary, in order to conduct these assessments.

(b) Once completed, the facility or site ATO will notify the respective DRO ATO the annual MARMs review or update is available.

(c) In addition to MARMS, the ATPR will also include reviewing/evaluating the following, to assess operability, identify gaps in operational procedures, refine policies, and create recommendations for program improvements:

1. ATP.
2. Security Incidents.
3. Training, Drills, and Exercises.
4. AT-related projects.

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

(e) AT Assessments will be conducted using applicable DoD-approved benchmarks, Interagency Security Committee, and Unified Facilities Criteria standards, as well as guidance from the GCC, host, or parent installation in which the DHA sites/facilities operate.

(f) HHQ assessments will be conducted triennially by the DHA Security Branch inspection team. DHA will coordinate with each respective DRO Director office to establish a schedule, to include identifying personnel to assist with conducting the assessments, as needed.

(g) When possible, ATPRs will be conducted in conjunction with VAs (Reference (h)).

8. RANDOM AT MEASURES

a. Objective. Protection of DHA personnel and assets from acts of terrorism is one of the most complex challenges for all Facility Directors, DOs, SOs, or SAOs. Planning to confront this challenge requires a comprehensive, integrated approach. References (d) and (e) provide the AT/FP requirements.

b. Intent. RAMs are tools that assist Facility Directors, DO, or SO with complementing (enhancing) and supplementing – but not replacing – mandated physical security requirements.

RAMs allow DHA to enhance security, break patterns, and vary responses to threats. RAMs are meant to be utilized in a collective, proactive effort focused on the prevention and detection of terrorist attacks against DHA personnel and their families, sites, facilities, installations, and infrastructure critical to mission accomplishment.

c. Implementation. RAMs may include ID card checks, limiting facility access to single entrances, and similar measures. RAMs are developed and implemented based upon general and specific threats.

(1) RAMs will be conducted at all DHA-administered sites, facilities, or GSA-leased spaces.

(2) DHA tenants of DoD installations will partner and liaise with the responsible installation AT office to identify, develop, and implement local RAMs not covered by DoD or GCC. GSFs will coordinate with their host or parent installation, GCC, and other appropriate agencies concerning the establishment and implementation of RAMs at all off-installation sites or facilities.

(3) The facility ATO will oversee implementation of RAMs at all DHA sites and facilities, including GSA-leased facilities or spaces.

(4) Facility Directors will ensure the implementation of RAMs are codified into their overall ATP.

(a) RAMs can be conducted by assigned military members, government employees, and contractors. NOTE: Contractors may be limited on conducting certain RAMs.

(b) RAM guidance will include minimum and maximum durations that RAMs will be conducted.

(c) If a required RAM cannot be conducted (e.g., lack of authority, jurisdiction, or not being applicable), Facility Directors, DOs, SOs, or SAOs are required to identify, conduct, and document a different RAM. Personnel must also document the original RAM information (e.g., RAM number) and the reason that RAM could not be conducted (e.g., interfere with joint training, no capability, authority).

(5) The facility ATO will consolidate and document all completed RAM information at the end of the month and forward the information to the host or parent installation AT Office or DRO ATO as appropriate.

9. FPCON. The FPCON system progressively increases protective measures implemented in anticipation of, or in response to, terrorist attack. FPCONs are the principal means through which DoD civilians and military commanders apply an operational decision to guarding against terrorist and other threats.

a. Authority, in accordance with Reference (e), the Unified Command Plan and in compliance with all applicable orders, guidance, and direction issued by the Secretary of Defense, GCC have the authority to declare FPCON levels throughout their respective AORs. Most DHA sites or facilities are located on host or parent installations, while others are considered GSFs that are assigned to (monitored and supported by) the nearest DoD installation. Therefore, Facility Directors, DO, or SO will ensure:

(1) DHA tenants located on or assigned to a host or parent installation adhere to the FPCON guidance and direction of the installation commander or GCC.

(2) GSFs, located off DoD installations adhere to FPCON guidance of their host or parent installation.

b. Any Facility Director, DO, or SO may add mandatory FPCON measures from higher FPCON levels, or add supplemental FPCON measures over those FPCON measures a GCC declares, based on the threat to their particular installation, separate facility, or operating area. However, Facility Directors, DO, or SO must notify the DRO ATO of these actions as soon as practical.

c. Facility Directors, DO, or SO do not have the authority to lower GCC-declared FPCON levels or cease FPCON measures without authorization from the GCC.

d. FPCON Action Sets are site-specific measures that will be taken to meet mandated FPCON requirements for protecting personnel, resources, and infrastructure. Facility Directors, DO, or SO must:

(1) Review the DoD and GCC mandated FPCON measures.

(2) Evaluate what is involved for implementation.

(3) Consider potential impacts to DHA personnel, mission, resources, and infrastructure.

(4) Coordinate with the host or parent installation and DHA HQ if necessary, concerning any issues, support requirements, etc.

(5) Develop and implement a plan to meet mandated FPCON measures.

(6) Review and update established FPCON Action Sets at least annually and when directed by higher authority.

10. SUSPICIOUS ACTIVITY (SA)/INCIDENT REPORTING. Threats (e.g., criminal activity, suspicious packages or objects, phone or email threats, bomb threats, fire, civil disturbance, hostage situations, active shooter, and suicide bombers) require actions by the Facility Director, DO, or SO, ATO/R, and DHA personnel.

a. SA/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.

b. On Military Installations. DHA sites/facilities located on military installations will report all SA, to include security-related incidents to the Facility Dispatch/Security Control Center; or host or parent installation security/law enforcement immediately if no dispatch/control center exists. NOTE: Many installations have a local emergency phone number, which should be used for fastest response. 9-1-1 or local emergency numbers can be utilized for any emergency if the installation emergency number is not unavailable, but might result in a delay while a 9-1-1 operator transfers the call to the installation. The Facility Dispatch/Security Control Center will then contact the host-installation security forces, who will respond, investigate and up-channel the report through the respective Installation Command Post in accordance with the appropriate Situation Report and OPREP category (i.e., OPREP 3) and procedures specified by Reference (o), Situational Monitoring Manual, or otherwise directed local procedure. Facility Directors, DO, or SO should identify, coordinate and establish additional support requirements via installation support plan, memorandum of agreement, etc., with host or parent installations.

c. Off Military Installations. For GSFs located off military installations, any threat indicators, SA, or security-related incidents need be reported to the Facility Dispatch/Security Control Center, security guard, or Designated Security Representative immediately. NOTE: 9-1-1 or local emergency numbers should be utilized for any emergency, since GSFs normally rely on local civilian responders rather than installation emergency responders. Dependent upon local installation support plans, memorandums of agreement, etc., the Facility Dispatch/Security Control Center, security guard, or Designated Security Representative will then notify FPS and/or local host or parent installation law enforcement concerning the incident.

d. Security Related Incidents. Facility Directors, DO, or SO will complete a DHA Notice of Security Incident, concerning all security-related incidents.

(1) Once completed, the notice of Security Incident should be submitted via Non-classified Internet Protocol Router Network to the respective DRO Director and courtesy copy DHA Security Branch at dha.physec@mail.mil within 24 hours of the incident.

(2) The subject of the email submission should be listed as "SI" (Security Incident) and include the site/facility and the date the incident occurred (i.e., SI – DHHQ – 20210514).

11. WORKPLACE VIOLENCE. There is significant crossover between workplace violence and terrorism motivations, indicators, prevention, and response. DHA implements the DoD workplace violence prevention and response policy through Reference (r). An effective workplace violence prevention program can significantly benefit the AT program. See Reference (r) for detailed guidance.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AAR	After Action Review
AOR	Area of Responsibility – assigned to Geographic Combatant Commanders as specified in the Unified Command Plan
AT	Antiterrorism
ATEC	Antiterrorism Executive Committee
ATO	Antiterrorism Officer
ATO/R	Antiterrorism Officer/ Antiterrorism Representative
ATP	Antiterrorism Plan
ATPR	Antiterrorism Program Review
ATR	Antiterrorism Representative
ATWG	Antiterrorism Working Group
CA	Criticality Assessment
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosive
COA	courses of action
DCA	Defense Critical Assets
DHA	Defense Health Agency
DHA-AI	Defense Health Agency-Administrative Instruction
DO	Designated Official
DRO	Direct Reporting Organization
EOP	Emergency Operations Plan
EPRM	Enterprise Protection Risk Management
E-W	enterprise-wide
FP	Force Protection
FPCON	Force Protection Condition
FPS	Federal Protective Services
GCC	Geographic Combatant Commander
GSF	geographically separated facilities
HHQ	Higher Headquarters
HQ	Headquarters
ID	Identification
MARMS	Mission Assurance Risk Management System
MOA	memorandums of agreement

OEP	Occupant Emergency Plan
OPREP	Operational Reports
PFPA	Pentagon Force Protection Agency
PPBE	Planning, Programming, Budgeting, and Execution
RA	Risk assessment
SA	suspicious activity
SAO	Senior Agency Official
SO	Senior Official
TA	threat assessment
TCA	Task Critical Assets
TWG	Threat Working Group
USNORTHCOM	United States Northern Command
VA	vulnerability assessment
WMD	Weapon of Mass Destruction

PART II. DEFINITIONS

AT. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces.

AT Awareness. Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorism.

ATO. The principal military or civilian advisor charged with managing the AT program for the Military Commander or DoD civilian exercising equivalent authority.

AT planning. The process of developing specific guidance and execution-oriented instructions for subordinates. An ATP contains command-specific guidance for the establishment of an AT Program and the implementation of the AT standards prescribed.

AT Program Review. A systematic, comprehensive assessment of the AT Program against the written DoD standards prescribed.

AT risk management. The process of systematically identifying, assessing, and controlling risks arising from operational factors and making decisions that balance possible adverse outcomes with mission benefits. AT risk management is one of the five minimum elements of an AT program. The end products of the AT program risk management process will be the ID of DoD elements and personnel that are vulnerable to the identified threat attack means. From the

assessment of risk based upon the three critical components of AT risk management (TA, CA, and VA), the commander or DoD civilian manager or director must determine which DoD elements and personnel are at greatest risk and how best to employ given resources and FP measures to deter, mitigate, or prepare for a terrorist incident.

CA. Identifies key assets and infrastructure that support DoD missions, units, or activities and are deemed mission critical by Military Commanders or civilian agency managers. It addresses the effect of temporary or permanent loss of key assets or critical infrastructures on the installation or a unit's ability to perform its mission.

consequence management. Those measures taken to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of a CBRNE situation.

crisis management. Measures to identify, acquire, plan, and use the resources needed to anticipate, prevent, and resolve a threat or act of terrorism. Crisis management is predominately a law enforcement function.

critical asset. Any facility, equipment, service, or resource considered essential to DoD operations in peace, crisis, and war, warranting measures of precautions to ensure its continued efficient operations, protection from disruption, degradation, or destruction, and its timely restoration. Critical assets may be DoD assets or other government or private assets, (e.g., industrial or critical infrastructure assets), domestic or foreign, the disruption or loss of which could render DoD critical assets ineffective or otherwise seriously disrupt DoD operations.

critical infrastructure. Infrastructure deemed essential to DoD operations or the functioning of a critical asset.

delegated/non-delegated facility. A delegated leased facility where the General Services Administration may, by agreement with occupant agencies, delegate authority to perform specified functions with respect to the operation, maintenance, or repair of General Services Administration assigned space. A DoD-delegated facility is a facility for which DoD has been delegated such authority. A non-DoD-delegated facility is a facility for which DoD has not been delegated such authority.

Direct Reporting Organizations. Direct Reporting Medical Treatment Facility, Small Market and Stand-Alone Military Medical Treatment Facility Organization, and DHA Regions reporting to the DHA.

DoD contractor. Any individual firm, corporation, partnership, association, or other legal non-federal entity that enters a contract directly with the DoD to furnish services, supplies, or both, including construction. DoD contractors may include U.S. Nationals, local citizens, or third country nationals. Foreign governments, representatives of foreign governments, or foreign corporations wholly owned by foreign governments that have entered into contracts with the DoD are not DoD contractors.

DoD personnel. Unformed military active duty and reserve members and DoD federal civilian employees hired and paid from appropriated and non-appropriated funds under permanent or temporary appointment.

elements and personnel. Military and civilian personnel and their dependent family members; DoD installations and facilities; DoD-owned, leased, or managed infrastructure and assets critical to mission accomplishment; and other DoD-owned, leased, or managed mission essential assets.

Emergency Responder. Firefighters, law enforcement/security forces, and emergency medical technicians, emergency management and operations personnel, Explosive Ordinance Disposal personnel, physicians, nurses, medical treatment providers at DHA facilities, disaster preparedness officers, public health officers, bio-environmental engineers, and mortuary affairs personnel.

facilities. To include all Military Treatment Facilities, Dental Treatment Facilities, and Veterinary Treatment Facilities

family member. Individuals defined as “Dependent” in Reference (h). Includes spouses; unmarried widows; unmarried widowers; unmarried legitimate children, including adopted children or stepchildren, who are under 21, incapable of self-support, or under 23 and enrolled in a fulltime institution of higher learning. In addition, the family members of DoD civilian employees, particularly as it pertains to those assigned overseas. The DoD standard for family members requiring Level 1 AT Awareness Training is 14 years or older (or younger at the discretion of the DoD sponsor).

FP. Preventive measures taken to mitigate hostile actions against DoD personnel and family members, resources, facilities, and critical information. These actions conserve the force’s fighting potential, so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the Joint Force while degrading the opportunities of the enemy. FP does not include actions to defeat the enemy or protect against accidents, weather, or disease.

FPCON. A Chairman of the Joint Chiefs of Staff-approved standard for ID of and recommended responses to terrorist threats against U.S. personnel and facilities. The system is the principal means for a commander to apply an operations decision on how to protect against terrorism and facilitates coordination among DoD Components and support for AT activities.

High Risk Personnel. Personnel, who by their grade, assignment, symbolic value, or relative isolation, are likely to be an attractive or accessible terrorist targets.

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.

security. (a) Measures taken by a military unit, activity, or installation, to protect itself against all acts designed to, or which may, impair its effectiveness; (b) a condition that results from establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

special event. An activity characterized by a large concentration of personnel and/or a gathering where distinguished visitors are involved, often associated with a unique or symbolic event.

terrorism. The unlawful use of violence or threat of violence often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political.

terrorism consequence management. DoD preparedness and response for mitigating the consequences of a terrorist incident including the terrorist use of a WMD. DoD consequence management activities are designed to support the lead federal agency, the Department of Homeland Security, and include measures to alleviate damage, loss of life, hardship, or suffering caused by the incident; protect public health and safety; and restore emergency essential government services.

terrorism threat analysis. In AT, a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target the DoD Components or the DoD elements and personnel. A terrorism threat analysis is an essential step in identifying the probability of terrorist attack(s) and results in a terrorism TA.

TA. (a) The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat, or (b) the product of a threat analysis for a particular unit, installation, or activity.

terrorist incident response measures. A set of procedures established for response forces to deal with the effects of a terrorist incident.

terrorist threat level. A Department of Defense intelligence TA of the level of terrorist threat faced by U.S. personnel and interests. The assessment is based on a continuous intelligence analysis of a minimum of four elements: terrorist group operational capability, intentions, activity, and operational environment. There are four levels: LOW, MODERATE, SIGNIFICANT, and HIGH. Threat levels should not be confused with FPCON. Terrorism TAs are provided to senior leaders to help them determine the appropriate FPCON.

VA. A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility, or other site to a terrorist attack. It identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. The process the Commander uses to determine the susceptibility to attack from the full range of threats to the security of personnel, family members, and facilities, which provide a basis for determining AT Measures that can protect personnel and assets from terrorist attacks.

vulnerability. (a) In AT, a situation or circumstance, which if left unchanged, may result in the loss of life or damage to mission essential resources; (b) the susceptibility of a nation or a military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished; (c) the characteristics of a system that can cause it to be degraded (incapability to perform the designated mission) as a result of being subjected to a certain level of effects in an unnaturally (manmade) hostile environment.

WMD. CBRNE weapons capable of a high order of destruction or causing mass casualties, excluding the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon.