



**Joint Staff / Defense Threat Reduction Agency  
DOD Vulnerability Assessment Benchmarks  
January 1, 2009**

**DISTRIBUTION STATEMENT C: Distribution authorized to U.S. Government Agencies and their contractors. Administrative/Operational Use; 1 Sep 03. Other requests for this document shall be referred to the Defense Threat Reduction Agency, 8725 John J. Kingman Road, MSC 6201, Fort Belvoir, VA 22080-6201.**

**This document contains FOUO information exempt from mandatory disclosure under the FOIA. Exemption (b) (2) high applies.**

Annex A: Terrorist Operations	Page 2 - 14
Annex B: Security Operations	Page 15 - 55
Annex C: Structural Engineering	Page 56 - 69
Annex D: Infrastructure Engineering	Page 70 - 86
Annex E: Emergency Management	Page 87 - 117

**FOR OFFICIAL USE ONLY**

**Annex A  
Terrorist Operations Benchmarks**

<b>1. AT RISK MANAGEMENT</b>		
TO-RM-01	<p><b>Risk Management.</b> The AT Risk Management process shall be performed IAW HHQ guidance and its products reviewed annually. Risk management will be applied in all aspects of AT Program implementation and planning, including operational plans and decisions, development of risk mitigation measures, and prioritization and allocation of resources.</p> <ul style="list-style-type: none"><li>• Does the installation's AT Program outline a process to conduct AT Risk Management?</li><li>• Does the AT Risk Management process:<ul style="list-style-type: none"><li>○ Identify / characterize threats?</li><li>○ Identify assets / loss impacts?</li><li>○ Identify / analyze vulnerabilities?</li><li>○ Assess risk / determine priorities for asset protection?</li><li>○ Identify countermeasures / costs / trade-offs?</li><li>○ Develop controls / make risk decisions?</li><li>○ Implement controls?</li><li>○ Address supervision / review?</li><li>○ Include residual risk identification?</li></ul></li><li>• Is a person or entity assigned for supervising the integration of Risk Management across the entire AT Program?</li></ul>	DOD Std 3  JP 3-07.2, Ch. I  DOD O-2000.12-H, Chapter 4  DOD O-2000.12-P,  Strategic Goal 1H  FM 3-100.12

## FOR OFFICIAL USE ONLY

TO-RM-02	<p><b>Threat Assessment.</b> A terrorism threat assessment (TA) shall be developed and conducted annually IAW HHQ guidance. The TA is a product of terrorism threat analysis. Terrorism threat analysis is defined as the continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups or individuals that could target DOD components, elements, and personnel.</p> <ul style="list-style-type: none"> <li>• Is the TA current?</li> <li>• Is the TA updated annually or more frequently as the terrorist threat environment dictates?</li> <li>• Does the TA use the DOD Terrorism Threat Analysis Methodology? (Operational Capability, Intentions, Activity, Operating Environment)             <ul style="list-style-type: none"> <li>○ Is the DIA-identified threat level used by the installation? [Installation commanders cannot set their own Threat Level] (DOD Std 2)</li> <li>○ If different than the DIA threat level, did the COCOM set the threat level? (if applicable)</li> </ul> </li> <li>• Does the TA use the Defense Threat Assessment (DTA) Format?</li> <li>• Does the TA identify the full range of feasible (known or estimated) terrorist capabilities (weapons, tactics, techniques, and methods of attack)?</li> <li>• Does the TA assess the terrorist threat for probability and severity of occurrence? [Threat matrix is a good tool for identifying capabilities, probability, and severity, but it is not a requirement]</li> <li>• Are feasible chemical, biological, nuclear, radiological, and high-yield explosives (CBRNE) / weapons of mass destruction (WMD) threats identified? The COCOM, Service, or Defense Agency CBRNE / WMD TA can be integrated into the Local TA (LTA) to meet this requirement.</li> <li>• Is there a process to integrate and fuse all source information? [strategic, operational, and tactical (local) intelligence products]             <ul style="list-style-type: none"> <li>○ Strategic - DIA, CIA, DOJ, DOS, NSA, DHS</li> <li>○ Operational – Services (Army Counterintelligence Center (ACIC), Naval Criminal Investigative Service (NCIS), Air Force Office of Special Investigations (AFOSI), COCOM J-2s and Intelligence Centers</li> <li>○ Local, state, federal (FBI), and host-nation law enforcement agencies?</li> <li>○ Appropriate local, state, federal, and host-nation Intelligence Community (IC) activities?</li> <li>○ Applicable U.S. country team; port authority officials and husbanding contractors?</li> </ul> </li> <li>• Is the assessment tailored to the local environment?</li> <li>• Is the TA integrated into the AT Program?             <ul style="list-style-type: none"> <li>○ Integrated into Risk Management?</li> <li>○ Justification for implementation of RAMs? [Coordinate with Security Operations.]</li> <li>○ Physical Security changes? [Coordinate with Security Operations.]</li> <li>○ Program and budget requests?</li> <li>○ Used when conducting VAs, especially the Design Basis Threat?</li> <li>○ Used as the basis to provide justification for changes to the FPCONs? (Review through the TWG and ATWG (Security Operations))</li> </ul> </li> <li>• Are specific TAs developed to support operational planning and risk decisions for unique mission requirements or special events including, but not limited to, training and exercises and special security events?</li> </ul>	<p>DOD Std 4</p> <p>JP 3-07.2, Ch III, VI, &amp; AP B</p> <p>DOD 2000.12 E4.1.16</p> <p>DOD O-2000.12-H, Chapter 5</p> <p>Strategic Goal 1E</p> <p>DODI 5240.18 dtd Dec 2006</p> <p>OUSD/CIS Memo Standardized DOD Threat Assessment dtd Dec 2003</p>
----------	--	---

**FOR OFFICIAL USE ONLY**

<p>TO-RM-03</p>	<p><b>Criticality Assessment.</b> A criticality assessment (CA) shall be established and updated annually IAW HHQ guidance.</p> <ul style="list-style-type: none"> <li>• Is the CA current?</li> <li>• Does the CA comply with HHQ guidance?</li> <li>• Has some mission analysis been conducted to identify mission critical assets using:             <ul style="list-style-type: none"> <li>○ DOD Directives – Universal Joint Task List (UJTLs)</li> <li>○ COCOM Directives – OPLANS, Joint Mission Essential Task List (JMETL)</li> <li>○ Service Directives – Mission Essential Task List (METL)</li> <li>○ Commander’s priorities</li> </ul> </li> <li>• Does the CA identify, classify, and prioritize mission-essential assets, resources, and personnel critical to mission accomplishment?             <ul style="list-style-type: none"> <li>○ Are COCOM, DOD Defense Infrastructure Sector Lead Agency, and other HHQ task critical assets included in the list of critical assets? (Criticality should be established by the COCOM or other mission / asset owner.)</li> </ul> </li> <li>• Are tenants’ critical assets included in the assessment?</li> <li>• Are CAs based upon relative importance, effect of loss, recoverability, mission functionality, substitutability, and reparability? [Tools for determining asset criticality: Criticality Assessment Matrix using importance, effect, recoverability, mission functionality, substitutability, and reparability; MEVA; JAT Guide; MSHARPP; and CARVER]</li> <li>• Does the CA address non-mission essential assets including high population facilities; mass gathering activities; and any other facility, equipment, service, or resource deemed important by the Commander and warranting protective measures?</li> <li>• Does the CA identify redundancies within critical functions?</li> <li>• Does the CA determine time required to duplicate key assets or infrastructure efforts if temporarily or permanently lost?</li> </ul>	<p>DOD Std 5</p> <p>JP 3-07.2, AP A - 1</p> <p>DOD O-2000.12-H, Chapter 6</p> <p>Strategic Goal 1F</p> <p>DODI 3020.45</p>
-----------------	---	--

## FOR OFFICIAL USE ONLY

<p>TO-RM-04</p>	<p><b>Vulnerability Assessment.</b> A vulnerability assessment (VA) shall be established and conducted annually IAW HHQ guidance.</p> <ul style="list-style-type: none"> <li>• Does the installation VA comply with HHQ guidance for local assessments? [Includes team, process, benchmarks, and frequency.] See Table E3.T1 of DODI 2000.16 for frequency.</li> <li>• Is the VA current? [Within the last 12 months.]</li> <li>• Does the VA include mission essential assets, resources, and personnel critical to mission success that are susceptible to a terrorist attack?</li> <li>• Does the VA include DOD owned or leased facilities that are NOT a tenant on an installation?</li> <li>• Does the VA include DOD day care, schools, and transportation routes? (Triennial requirement.)</li> <li>• Is the VA properly classified IAW DTRA Security Classification Guide or COCOM supplement?</li> <li>• Was the current TA used when conducting VAs, to include the local DBT?</li> <li>• Have the following actions been completed within 90 days of a completed VA:             <ul style="list-style-type: none"> <li>○ Vulnerabilities prioritized?</li> <li>○ Has a plan of action (immediate and final) been developed to mitigate or eliminate the vulnerabilities?</li> <li>○ Have the results of the VA been reported to first general officer, flag officer, or civilian equivalent director in the chain of command?                 <ul style="list-style-type: none"> <li>▪ Reporting of vulnerabilities may be accomplished by Core Vulnerability Assessment Management Program (CVAMP), written memorandum, or Defense Readiness Reporting System (DRRS). (See COCOM guidance.)</li> </ul> </li> </ul> </li> <li>• Are vulnerabilities being tracked until mitigated?             <ul style="list-style-type: none"> <li>○ Is CVAMP being used to track vulnerabilities?</li> <li>○ Have all (HHQ and local) assessment results been populated into CVAMP within 120 days from completion of the assessment? (This is a DOD standard; check COCOM standard/guidance.)</li> <li>○ Does the Commander review and approve all CVAMP entries either by ATEC forum, CVAMP, or personnel review?</li> </ul> </li> <li>• Has a designated person / staff / unit been identified to conduct / lead the assessments?             <ul style="list-style-type: none"> <li>○ Is the ATWG or similar organization used to perform/validate the VA?</li> </ul> </li> </ul>	<p>DOD Std 6</p> <p>JP 3-07.2 AP C-1</p> <p>DOD O-2000.12-H, Ch. 7 &amp; 14</p> <p>DTRA SCG Dtd May 2005</p> <p>Strategic Goal 1G</p>
-----------------	--	---

**FOR OFFICIAL USE ONLY**

<p>TO-RM-05</p>	<p><b>Risk Assessment.</b> A risk assessment (RA) shall be established and conducted annually as part of the risk management process.</p> <ul style="list-style-type: none"> <li>• Does the RA comply with HHQ requirements? <ul style="list-style-type: none"> <li>○ Is the Joint Antiterrorism (JAT) Guide used?</li> <li>○ Is DOD O-2000.12-H, Chapter 8 used?</li> <li>○ Is CVAMP used? (SG 4D)</li> <li>○ (Any of these three programs satisfy the requirement for a RA product)</li> </ul> </li> <li>• Is data from the most recent TA, CA, and VA included in the RA?</li> <li>• Have countermeasures been identified to reduce the risk?</li> <li>• Has a cost-benefit analysis been conducted on the countermeasure?</li> <li>• Has a plan of action been developed to implement the countermeasures? <ul style="list-style-type: none"> <li>○ Does the countermeasure deter, detect, delay, deny / defend, defeat / destroy?</li> </ul> </li> <li>• Does the RA identify the amount of risk reduction gained by countermeasure implementation?</li> <li>• Has the RA been translated into action items for either resourcing or procedural corrections? (This can also be done using CVAMP.)</li> <li>• Have waivers been requested when risk is accepted (if required)?</li> <li>• Is there a prioritization method that assists the Commander with risk acceptance?</li> <li>• Have compensatory measures been identified for all risks that are accepted?</li> <li>• Was residual risk indentified to the Commander after implementing all available controls?</li> <li>• Is the RA conducted annually?</li> </ul>	<p>DOD Std 3</p> <p>JP 3-07.2 AP D-1</p> <p>DOD O-2000.12-H, Chapter 8</p> <p>Strategic Goal 1H</p> <p>FM 3-100.12</p>
<p>TO-RM-06</p>	<p><b>Design Basis Threat (DBT).</b> The installation shall establish and incorporate a DBT, which is promulgated as a planning factor for the installation’s physical security system. The DBT is the threat against which assets must be protected and upon which the protective system’s design is based.</p> <ul style="list-style-type: none"> <li>• Has the installation identified a DBT?</li> <li>• How was the DBT developed? <ul style="list-style-type: none"> <li>○ HHQ Directed</li> <li>○ Unified Facilities Criteria (UFC)</li> <li>○ Locally developed using threat analysis, TA, and threat matrix. (Must meet / exceed UFC / HHQ-directed DBT)</li> <li>○ Threat Matrix</li> </ul> </li> </ul>	<p>DOD Std 4</p> <p>JP 3-07.2, Chapter VI-14</p> <p>TM 5-853, Security Engineering</p> <p>UFC 4-020-01; 4-010-02</p>

**FOR OFFICIAL USE ONLY**

<b>2. AT PLANNING</b>		
TO-PLN-01	<p><b>Intelligence Support to the AT Program.</b> AT Intelligence shall be included in the AT Program and discussed in the intelligence annex of the AT Plan.</p> <p><b>PLANNING AND DIRECTION (TO-PLN-01A)</b></p> <ul style="list-style-type: none"> <li>• Has the Commander tasked the appropriate organization under their command or control to gather, analyze, and circulate appropriate terrorism threat information? (Note: If so designated, the TWG satisfies this requirement.)</li> <li>• If no organic intelligence capability exists, has the Commander arranged for intelligence support from either HHQ or other entity?</li> <li>• Does the AT Plan include an AT Intelligence Annex?</li> <li>• Have Commander’s Critical Information Requirements (CCIR) and Priority Intelligence Requirements (PIR) been developed to focus collection and analysis efforts?               <ul style="list-style-type: none"> <li>○ Are applicable COCOM, Military Departments, Defense Agencies, and Field Activities CCIRs and PIRs incorporated? (Including terrorist capability to acquire and use WMD.)</li> <li>○ Have FBI and DHS PIR been considered? (USNORTHCOM)</li> <li>○ Have factors that are associated with indicators and warnings of increased terrorist activity been defined?</li> </ul> </li> <li>• Has an entity been identified to provide Counterintelligence support for combating terrorism?</li> <li>• Has Counterintelligence support been integrated into the installation’s AT Program?               <ul style="list-style-type: none"> <li>○ DOD RM process?</li> <li>○ Terrorist TTP?</li> <li>○ Surveillance, Surveillance Detection, Countersurveillance?</li> <li>○ Legal aspects of Force Protection?</li> <li>○ Route analysis?</li> </ul> </li> </ul> <p><b>COLLECTION (TO-PLN-01B)</b></p> <ul style="list-style-type: none"> <li>• Has an AT threat information organization matrix/plan been developed based on information requirements?               <ul style="list-style-type: none"> <li>○ Has the Commander tasked an official to develop and maintain the AT threat information organization matrix / plan?</li> <li>○ Does the AT threat information organization matrix / plan include all PIRs and CCIRs?</li> <li>○ Do tasked organizations know they are tasked and understand reporting procedures?</li> <li>○ Is liaison activity defined?</li> </ul> </li> <li>• Are sources of strategic, operational, and tactical intelligence products identified?</li> <li>• Does the installation use the process identified by HHQ for requesting information? (Includes the development and handling of information / intelligence requirements.)</li> </ul> <p><b>PROCESSING AND EXPLOITATION (GENERALLY NOT USED) (TO-PLN-01C)</b></p>	<p>DOD Std 2 E4.4.2.10</p> <p>JP 3-07.2 AP B, E, K &amp; Fig K-1</p> <p>DOD O-2000.12-H, Chapter 5, 11 &amp; AP 4</p> <p>JP 2-0 Joint Intelligence dtd June 2007</p> <p>JP 2-01.3 Joint TTP for Joint IPB</p> <p>FM 34-2</p> <p>FM 34-130</p>

**FOR OFFICIAL USE ONLY**

	<p><b>PRODUCTION (TO-PLN-01D)</b></p> <ul style="list-style-type: none"> <li>• What intelligence products are produced locally? (May include threat assessments, threat matrix, indicators and warnings, AT articles, and special assessments.)</li> <li>• Is Intelligence Preparation of the Operational Environment (IPOE) conducted based on the developed DBT to develop terrorist courses of action (COA)?</li> </ul> <p><b>DISSEMINATION (TO-PLN-01E)</b></p> <ul style="list-style-type: none"> <li>• What is the process the Commander uses to forward up and down the chain of command all information pertaining to suspected terrorist threats or acts of terrorism involving personnel or assets for which they have responsibility? (e.g., suspicious activity reporting, Defense Terrorism Warning Reports, and/or HHQ threat messages, OPREP-3, Blue Dart, etc.)             <ul style="list-style-type: none"> <li>○ What are the methods of transmittal?</li> <li>○ Is the TWG/ATWG involved in this process?</li> <li>○ Is a dissemination process in place to transmit threat information to appropriate personnel / commands, specifically security forces personnel? [Verify with Security Operations]</li> <li>○ Is a process in place to notify the command when threat information is obtained?</li> </ul> </li> <li>• Are intelligence, CI, and law enforcement elements disseminating information on U.S. persons in support of AT Program implementation within the provisions of DODD 5200.27 and DOD 5240.1-R?</li> </ul>	
TO-PLN-02	<p><b>ATO SIPRNet Access.</b> The designated installation ATO shall have access to SIPRNET to receive classified intelligence information, provide AOR-specific briefs, and to main currency in AT Program updates from DOD, COCOM, and Service / Component Command.</p> <ul style="list-style-type: none"> <li>• Does the ATO have an Antiterrorism Enterprise Portal (ATEP) account?</li> <li>• Does the ATO belong to communities affiliated with his/her COCOM and Service/Component Command? (Not a requirement.)</li> </ul>	DOD Std 26  Strategic Goal II

**FOR OFFICIAL USE ONLY**

TO-PLN-03	<p><b>Threat Working Group.</b> A Threat Working Group (TWG) shall be identified as the focal point for integration of terrorist intelligence into AT operations.</p> <ul style="list-style-type: none"><li>• Does the plan address composition, charter, and responsibilities, including:<ul style="list-style-type: none"><li>○ Development and refinement of the terrorism threat assessment?</li><li>○ Assessing probability and severity of occurrence?<ul style="list-style-type: none"><li>▪ Threat Matrix can be used.</li></ul></li><li>○ Establishing the local DBT (if required)?</li><li>○ Coordination and dissemination of threat warnings, reports, and summaries?</li></ul></li><li>• Does the TWG integrate threat information derived from intelligence and counterintelligence sources with reports of criminal or suspicious activity derived from local law enforcement, the military community, or other sources?<ul style="list-style-type: none"><li>○ Does the TWG identify mitigation courses of action for identified threats?</li><li>○ Is the process for issuing threat warnings in place?</li><li>○ Are reviews conducted when the threat changes?</li><li>○ Do regularly scheduled meetings occur (quarterly), as threat activity dictates, or based on COCOM or AT Plan requirements?</li></ul></li><li>• Are minutes kept for each meeting and are they disseminated?</li><li>• Is actionable information provided to the ATWG or similar activity?</li></ul>	DOD Std 11  DOD O-2000.12-H, Ch. 1.2.5  Strategic Goal 1B
-----------	---	---

**FOR OFFICIAL USE ONLY**

<p>TO-PLN-04</p>	<p><b>Surveillance Detection / Counter-surveillance.</b> The installation AT programs shall integrate counter-surveillance (CS) and surveillance detection (SD) as a matter of routine.</p> <ul style="list-style-type: none"> <li>• Is there a program identified for CS and SD?</li> <li>• Are organic capabilities/tasks identified in the AT Plan?             <ul style="list-style-type: none"> <li>○ If no organic capability exists, has the Commander arranged for support from either HHQ or other entity?</li> </ul> </li> <li>• Has a SD program been developed?             <ul style="list-style-type: none"> <li>○ Does the SD program address the following elements:                 <ul style="list-style-type: none"> <li>▪ Threat identification?</li> <li>▪ Modes and methods of surveillance?</li> <li>▪ Identification of surveillance requirements?</li> <li>▪ Identification of hostile surveillance locations?</li> <li>▪ Reporting and fusion process?</li> <li>▪ Command education?</li> </ul> </li> </ul> </li> <li>• Have fixed point surveillance diagrams been developed and shared with security forces, tenant commands, and housing offices? (not a requirement; best practice if developed.)</li> <li>• Have procedures for reporting and investigating possible surveillance been developed?             <ul style="list-style-type: none"> <li>○ What reporting system is used? (FBI's GUARDIAN REPORTING SYSTEM for CONUS/OCONUS COCOM directed.) (SG 1A)</li> </ul> </li> <li>• Have the following procedures for the neutralization and exploitation of surveillance been developed?             <ul style="list-style-type: none"> <li>○ Liaison.</li> <li>○ LE / CI Support.</li> <li>○ Responses, including RAMSs, FPCON increases, and awareness briefs.</li> </ul> </li> <li>• Does the SD program address a process to request specialized countersurveillance assets from HHQ?</li> <li>• Are individuals trained to identify/report potential terrorist surveillance?</li> <li>• Does the installation have a community watch program? If so, are reporting procedures known throughout the community?</li> </ul>	<p>DOD Std 2 E3.2.2.4.</p> <p>JP 3-07.2, Chapter III</p> <p>DOD O-2000.12-H, AP 7</p>
------------------	--	---

**FOR OFFICIAL USE ONLY**

<p>TO-PLN-05</p>	<p>The installation shall establish a Website Vulnerability Review Program to ensure that inadvertent or unauthorized disclosure of sensitive information via the world wide web is protected.</p> <ul style="list-style-type: none"> <li>• Has responsibility for the Website Vulnerability Review Program been assigned? (This could be the installation PAO / OPSEC Manager.)</li> <li>• Have procedures and guidelines been established for information provided on the DOD websites that are publicly accessible?</li> <li>• Are all stakeholders involved in the review process? (e.g., Webmasters, page maintainers, network administrators, SMEs, PAOs, and OPSEC personnel.)</li> <li>• Do evaluations of activity information follow current OPSEC procedures?</li> <li>• How often are website reviews conducted?</li> <li>• Are website reviews based on established critical information?</li> </ul>	<p>DOD Std 7 E4.4.3.18.</p> <p>DOD O- 2000.12-H Chapter 20</p> <p>DODD 5230.9</p> <p>DODI 5230.29</p> <p>DOD Manual 5205.02 DOD OPSEC</p> <p>JP 3-13.3</p> <p>DOD Website Admin Policies &amp; Procedures Nov 98 / Jan 02</p> <p>AR 25-1 AFI 35-101, Ch 1 SECNAV INSTR 5720.47B</p>
------------------	---	---

## FOR OFFICIAL USE ONLY

<b>3. AT RESOURCE APPLICATION</b>		
TO-RA-01	<p>AT resource requirements shall be based on risk management products.</p> <ul style="list-style-type: none"> <li>• Does the installation's AT resourcing process use risk analysis (criticality, threat, and vulnerability) products for resource determination?</li> <li>• Is there a resource justification / prioritization process that incorporates the following? (Review CVAMP)                             <ul style="list-style-type: none"> <li>○ Threat</li> <li>○ Asset criticality</li> <li>○ Asset vulnerability</li> <li>○ Current AT effectiveness</li> <li>○ Impact on Plan / Program</li> <li>○ Mitigation measures</li> <li>○ Commander's risk</li> </ul> </li> <li>• Have critical and high risk vulnerabilities been mitigated through funding decisions? [Requires thorough review of VA documents and CVAMP.]</li> </ul>	<p>DOD Std 3</p> <p>JP 3-07.2 AP C-1</p> <p>Strategic Goal 4F</p>
TO-RA-02	<p>The TO will review the following benchmark in support of the DOD Antiterrorism Strategic Plan and the SO assessment process. Findings from this benchmark will be provided to the Security Operations Specialist for the outbrief and written report.</p> <p>The Heads of DOD components shall submit prioritized AT requirements, to include those submitted or considered for CbT-RIF, to the Joint Staff J-3 DD AT/HD on an annual basis pursuant to current DOD Program Objective Memorandum (POM) guidance and timelines using CVAMP. The Risk Assessment portion of CVAMP must be filled out before funding can be submitted.</p> <ul style="list-style-type: none"> <li>• Is CVAMP used IAW HHQ guidance?</li> <li>• Is funding coded with CbT-RIF, UFR, or local funding?</li> </ul>	<p>DOD Std 30 E3.30.1.3.</p> <p>Strategic Goal 4D</p>
<b>4. ILLUSTRATIVE TARGET</b>		
	<p>Potential / sample targets shall be identified and evaluated. Targets shall be selected from a terrorist's viewpoint based on the implemented AT measures / security posture of the installation. Targeting will be based on the Defense Intelligence Agency's established terrorist threat level. Scenarios will be modeled after terrorist groups that are identified as having a presence in the Geographic Combatant Commander's AOR. This model focuses on the terrorist groups' operational capability and intentions. Targets may include non-mission essential assets, mission essential vulnerable areas, and critical infrastructure attacks. Targets will be used to exemplify the installation's vulnerabilities against commonly used terrorist weapons and tactics as well as CBRNE. The scenario must exploit vulnerabilities identified.</p>	

**FOR OFFICIAL USE ONLY**

<p>TO-IT-01</p>	<p>During the targeting portion of the assessment, observations will made by the TO identifying critical information and actions which can be observed by a terrorist that can be interpreted or pieced together to assist in targeting. This will include:</p> <ul style="list-style-type: none"> <li>• Publicly available documents produced by the installation should not contain information that can be exploited by a terrorist organization. These documents include the installation’s web site, newspapers, etc.</li> <li>• Observations made by the Terrorist Operations Specialist that identify vulnerabilities on the installation that can be exploited by a terrorist organization. These observed vulnerabilities may or may not be associated with the targets selected as illustrative targets.</li> </ul>	
<p>TO-IT-02</p>	<p>To develop Terrorist COAs, a systematic approach that addresses timelines and processes used by terrorist organizations must be used. A postulated terrorist attack event cycle is the basic standard by which this process can be accomplished.</p> <p>This terrorist attack cycle consists of five distinct steps, culminating in the actual attack. These steps have been identified as:</p> <p>1) Target Selection: This phase initiates the Operational Cycle Timeline. During this phase, potential targets are chosen. When developing terrorist COAs, the TO should identify those factors that would make the command a terrorist target. This may include recent news reporting, symbolism, location, etc.</p> <p>2) Surveillance: Potential targets are placed under surveillance to determine the final target. During this phase, the cell members collect planning information that will drive requirements. While more intelligence collection will often occur later, during this early step cell members will:</p> <ul style="list-style-type: none"> <li>• Perform a general reconnaissance of the target(s) visually, supplemented with still and video photography.</li> <li>• Video capability may include downloading to a personal computer for immediate or later transmission.</li> <li>• Notes may be taken, strip maps drawn, or maps marked.</li> <li>• During this stage, the TO should identify hostile surveillance locations and evaluate open source material to determine what information can be collected that would aid a terrorist organization in planning an attack against the command.</li> </ul>	

## FOR OFFICIAL USE ONLY

	<p>3) Attack Planning and Preparation: Surveillance assessment data is evaluated and analyzed to identify the target. This is a key point in the Operational Cycle Timeline during which all data is assimilated and a specific target is selected. After developing a list of potential targets, a process such as MSHARPP or CARVER is used to select a particular target. Specifics of the attack are determined. In this step, the tactical target is clearly defined. The target and surrounding area are now the object of a detailed reconnaissance to determine vulnerabilities (gaps and seams) and to identify the target's security measures, defenses, and potential obstacles that might hinder approach and egress. During this phase, the TO will identify the weapon and tactic that is to be used, describe the delivery method, describe the desired effects of the attack, and identify the vulnerabilities that were exploited in order to commit the act.</p> <p>4) Training and Deployment: Prior to deployment of the terrorist attack element, surveillance is conducted to verify information collected during surveillance and to familiarize the attackers with the attack plan. It is during this step that a final surveillance of the target may occur to determine whether any last minute security procedures have been put into place (Jersey barriers, police, etc.) If there is no change to the information, the terrorist attack element will deploy to the selected attack site for execution of the plan. If there are changes, terrorists will be forced to abandon or amend their plan.</p> <p>5) Attack: The type of attack (close-in or stand-off) as well as the attack site and timing are predicated on the information gathered by the terrorists in steps two and five, and must offer plausible opportunity for success.</p>	
--	---	--

**FOR OFFICIAL USE ONLY**

**Annex B  
Security Operations Specialist Benchmarks**

<b>1. AT RISK MANAGEMENT</b>		
SO-RM-01	<p><b>Personal Security Vulnerability Assessment (PSVA).</b> Installation commanders shall complete a PSVA for each person designated as High Risk Personnel (HRP). These processes shall be consistent with the HHQ directed procedures.</p> <ul style="list-style-type: none"> <li>• Does the installation have a process to conduct PSVAs for HRPs?</li> <li>• Are PSVAs completed within 90 days of assignment to the High Risk Billets (HRB)?</li> <li>• Are PSVAs revalidated annually and updated if the Terrorism Threat Level changes or at least every three years?</li> <li>• Do the PSVAs conform to the Defense Criminal Investigative Office formats?</li> </ul>	<p>DOD Std 6</p> <p>DOD 0-2000.12-H Chapter 7</p> <p>Strategic Goal 1G</p>
SO-RM-02	<p><b>Pre-deployment Vulnerability Assessments (PSVA).</b> Installation commanders shall complete PSVAs. Procedures must comply with the HHQ's guidance, such as frequency of assessments, time of VA, etc.</p> <ul style="list-style-type: none"> <li>• Is the installation's PSVA process conducted IAW the HHQ's guidance for air, sea, ground, and rail?</li> <li>• Are VAs conducted for the following:               <ul style="list-style-type: none"> <li>○ Sea, air, and ground movements?</li> <li>○ Assembly, staging, reception, and final bed down locations?</li> </ul> </li> <li>• Do in-transit and/or deployment VAs include assessments of critical roads and bridges?</li> <li>• Do pre-deployment VAs include movement or shipping of military cargo (including Military Sealift Command voyage charters)?</li> <li>• Are VAs conducted with enough time to allow proper time for the development of adequate security procedures and procure required resources (to include security augmentation if required)?</li> <li>• Did the VA include coordination with host nation for support?</li> <li>• Are previous VAs used to help support and establish / develop the current VA?</li> <li>• Is there a process established for deploying Commanders faced with emergent AT requirements to submit funding requests for the procurement of necessary equipment and materials to support the required AT posture?</li> <li>• What process are Commanders using to identify AT equipment and/or technology to their chain of command?</li> <li>• Are COTS and GOTS products used to meet near-term AT requirements?</li> </ul>	<p>DOD Std 6</p> <p>DOD 0-2000.12-H Chapter 7</p> <p>Strategic Goal 1G</p>

## FOR OFFICIAL USE ONLY

SO-RM-03	<p><b>Special Event Vulnerability Assessments.</b> Installation commanders shall ensure vulnerability assessments are conducted of any event or activity determined to be a special event or other activity involving a gathering of 300 or more DOD personnel.</p> <ul style="list-style-type: none"> <li>• Is there a process to ensure VAs of special events with 300 or more DOD personnel are accomplished?</li> <li>• Is the process for special events planning included in the AT Plan?</li> <li>• Are specific AT Plans or Operations Orders developed for each special event?</li> <li>• What is the process to monitor scheduling of special events?</li> <li>• Does the installation have a risk assessment process for special events? (Coordinate with terrorist options.)</li> </ul>	<p>DOD Std 6</p> <p>DOD 0-2000.12-H Chapter 7</p> <p>Strategic Goal 1G</p>
SO-RM-04	<p><b>Off-Installation Asset Vulnerability Assessments.</b> Installation commanders shall have a process to conduct vulnerability assessments of off-installation activities and facilities in areas where the Terrorism Threat Level is <b>SIGNIFICANT</b> or higher.</p> <ul style="list-style-type: none"> <li>• Are VAs conducted for off-installation housing areas? [Applicable in CONUS at DOD-owned or leased housing areas. Reference current USNORTHCOM OPORD.]</li> <li>• Do off-installation VAs, at a minimum, use the same DBT as the installation?</li> <li>• Are VAs conducted of DOD Dependent Schools located off the installation? [Reference DODEA AT Guidance.]</li> <li>• Are Daycare centers located off the installation included in the VA requirements?</li> <li>• Are VAs conducted on transportation systems used by DOD personnel and their family members, e.g. school buses, shuttle buses, etc?</li> <li>• Are VAs conducted on the routes of travel used by DOD personnel and their family members?</li> </ul>	<p>DOD Std 6</p> <p>DOD 0-2000.12-H Chapter 7</p> <p>Strategic Goal 1G</p>
<b>2. AT PROGRAM AND PLANNING</b>		
SO-PRO-01	<p><b>AT Program Elements.</b> The minimum required elements of a DOD AT Program shall be:</p> <ul style="list-style-type: none"> <li>• Risk Management (DOD Std 3)</li> <li>• Planning (including the AT Plan) (DOD Std 7)</li> <li>• Training and Exercises (DOD Std 23)</li> <li>• Resource Application (DOD 30)</li> <li>• Comprehensive Program Review (DOD Std 31)</li> <li>• Addresses all DOD Standards</li> <li>• Are these elements integrated into / support a comprehensive AT Program?</li> </ul>	<p>DOD Std 1</p> <p>DOD 0-2000.12-H Chapter 9</p> <p>Strategic Goal 2D</p>

**FOR OFFICIAL USE ONLY**

SO-PRO-02	<p><b>AT Program Coordination.</b> Installation commanders shall coordinate AT matters with local, state, federal, and host-nation authorities pursuant to existing law and DOD policy to support AT planning and program implementation.</p> <ul style="list-style-type: none"> <li>• Has the Commander coordinated the AT requirements with the local community?</li> <li>• Does coordination incorporate the information contained in the Country Memorandum of Agreement and the Status of Forces Agreement for OCONUS locations?</li> <li>• Does coordination include the ability to conduct FPCON measures that affect the local community?</li> <li>• Are tenants incorporated into the host installation's AT Program?</li> <li>• Are tenant security plans incorporated into the host's AT Program?</li> <li>• Is the senior DOD component responsible for integrating and coordinating security plans into a comprehensive installation or facility-wide AT program?</li> </ul>	<p>DOD Std 8</p> <p>DOD 0 2000.12-H Chapter 3</p>
SO-PRO-03	<p><b>Antiterrorism Officer (ATO).</b> The Installation Commander shall designate in a writing a Level II-certified commissioned officer, non-commissioned officer, or civilian staff officer as the installation's ATO. [ATO training is discussed in the Training and Exercise Section of these Benchmarks. (DOD Std 26)]</p> <ul style="list-style-type: none"> <li>• Has the Commander designated an ATO?</li> <li>• Is the ATO position a full time position?</li> <li>• Is an ATO designated at the battalion, ship, squadron, and separate facility level?</li> <li>• Is there an ATO assigned to deploying units with 300 or more personnel?</li> <li>• Is CBRNE expertise available to support the ATO (assigned on staff or supporting the program)? [This is a consideration.]</li> </ul>	<p>DOD Std 9</p> <p>DOD 0- 2000.12-H Chapter 9</p> <p>Strategic Goal 3C</p>
SO-PRO-04	<p><b>Antiterrorism Executive Committee (ATEC).</b> The Installation Commander shall establish an Antiterrorism Executive-level Committee or similarly structured corporate body at the installation and geographically separated facility level and higher (stationary or deployed).</p> <ul style="list-style-type: none"> <li>• Has the Installation Commander established an ATEC?</li> <li>• Does the ATEC meet at a minimum on a semi-annual basis?</li> <li>• Is the ATEC responsible for: <ul style="list-style-type: none"> <li>○ Developing and refining AT Program guidance, policy, and standards?</li> <li>○ Acting upon recommendations of the ATWG and TWG?</li> <li>○ Determining resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities?</li> </ul> </li> <li>• Is ATEC charter captured in AT Plan?</li> </ul>	<p>DOD Std 12</p> <p>Strategic Goal 2B</p>

**FOR OFFICIAL USE ONLY**

<p>SO-PRO-05</p>	<p><b>Antiterrorism Working Group.</b> The Installation Commander shall establish an Antiterrorism Working Group (ATWG).</p> <ul style="list-style-type: none"> <li>• Has the Installation Commander established an ATWG?</li> <li>• Does the ATWG meet at a minimum on a semi-annual basis or more frequently dependent upon the level of threat activity?</li> <li>• Is the ATWG responsible for:             <ul style="list-style-type: none"> <li>○ Developing and refining AT plans?</li> <li>○ Conducting VAs?</li> <li>○ Addressing emergent or emergency AT program issues?</li> <li>○ Prioritizing AT resource requirements?</li> </ul> </li> <li>• Are the right functions represented in the ATWG?             <ul style="list-style-type: none"> <li>○ Does the membership consist, of as a minimum:                 <ul style="list-style-type: none"> <li>▪ The Antiterrorism Officer?</li> <li>▪ Commander / civilian equivalent or designated representative?</li> <li>▪ Key members of the principle staff?</li> <li>▪ CBRNE expertise?</li> <li>▪ Tenant unit representatives?</li> <li>▪ Local and host-nation first responders (if appropriately cleared)?</li> </ul> </li> </ul> </li> <li>• Is the ATWG active? Does it keep minutes and accomplish the AT functions as defined in the AT Plan and DOD O-2000.12-H?</li> </ul>	<p>DOD Std 10</p> <p>Strategic Goal 2A</p> <p>DOD O-2000.12-H</p>
------------------	---	---

**FOR OFFICIAL USE ONLY**

	<b>AT PLAN</b>	
SO-PLN-01	<p><b>AT Plan.</b> The Installation Commander shall develop and maintain a comprehensive AT Plan for all DOD elements and personnel under their AT responsibility.</p> <ul style="list-style-type: none"> <li>• Is there an AT Plan that covers all personnel under the Commander’s AT responsibility?</li> <li>• Does the installation’s AT Plan address, as a minimum, the following applicable areas: <ul style="list-style-type: none"> <li>○ The minimum essential AT Program Elements (DOD Std 1)?</li> <li>○ Specific threat risk mitigation measures to establish a local baseline defensive posture? [Should incorporate the HHQ baseline.]</li> <li>○ AT Physical Security Measures (DOD Std 13)?</li> <li>○ AT Measures for Off-Installation Facilities, Housing, and Activities (DOD Std 15)?</li> <li>○ AT Measures for HRP (DOD Std 16)?</li> <li>○ AT Construction and Building Considerations (DOD Std 17)? [Coordinate with the Structural Engineer.]</li> <li>○ AT Measures for Logistics and Other Contracting (DOD Std 18)? [Coordinate with Infrastructure Engineer.]</li> <li>○ AT Measures for Critical Asset Security (DOD Std 19)? [Coordinate with all team members.]</li> <li>○ AT Measures for In-transit Movement?</li> <li>○ Terrorism Incident Response Measures (DOD Std 20)? [Coordinate with Emergency Management/CBRNE team members.]</li> <li>○ Terrorism Consequence Management Measures, including CBRNE and WMD mitigation planning (DOD Std 21)? [Coordinate with Emergency Management/CBRNE team members.]</li> <li>○ FPCON Implementation Measures, including Site-Specific AT Measures (DOD Std 22)?</li> <li>○ CBRNE Defense Joint Enabling Concepts of Sense, Shape, Shield, and Sustain per JROCM 180-3? [Coordinate with Emergency Management/CBRNE team members.]</li> </ul> </li> <li>• Has the AT Plan been tailored to the level of command and activity for which the AT principles were developed? [This includes the supporting plans.]</li> <li>• Has the AT Plan been signed and exercised?</li> <li>• Are AT Plans developed at the following levels beyond the installation-level: <ul style="list-style-type: none"> <li>○ Separate or leased facility/space?</li> <li>○ Ships?</li> <li>○ Operational deployments?</li> <li>○ Large scale Training and Exercises?</li> <li>○ Special events?</li> </ul> </li> </ul>	<p>DOD Std 7</p> <p>DOD O-2000.12-H Chapter 9</p> <p>Strategic Goal 2D</p>
	<b>FORCE PROTECTION CONDITION (FPCON) MEASURES</b>	
SO-PLN-02	<p><b>FPCON Measures.</b> Installation commanders shall establish policies and procedures for setting FPCON levels, FPCON transition, dissemination and implementation of FPCON measures, development of site-specific FPCON measures, and a waiver (exceptions) process for FPCON implementation (approved waivers shall be in writing, consistent with the guidelines in DOD O-2000.12-H.)</p>	<p>DOD Std 22</p> <p>DOD O-2000.12-H Chapter 10</p>

**FOR OFFICIAL USE ONLY**

	<p><b><u>SETTING FPCON LEVELS</u></b></p> <ul style="list-style-type: none"> <li>• Is the policy for setting FPCON levels promulgated in the AT Plan?</li> <li>• Are the ATWG and TWG involved in the FPCON setting process?</li> </ul> <p><b><u>FPCON TRANSITION</u></b></p> <ul style="list-style-type: none"> <li>• Has the installation established and published the process for transitioning between FPCON levels?</li> <li>• Does this process include lowering the FPCON Level and the implementation of supplemental measures and RAMs vice maintaining the higher level FPCON?             <ul style="list-style-type: none"> <li>○ Higher-level Commander’s FPCON level cannot be lowered without written concurrence.</li> </ul> </li> </ul> <p><b><u>FPCON DISSEMINATION AND IMPLEMENTATION</u></b></p> <ul style="list-style-type: none"> <li>• Has the installation established and published a process for disseminating and implementing FPCON measures?</li> <li>• Is there a process to determine that FPCON measures are implemented and maintained throughout the FPCON declaration?</li> <li>• Is there a process developed and prescribed for the notification of HHQ in regards to FPCON changes?</li> <li>• Are all mandated FPCON measures being implemented?</li> </ul> <p><b><u>FPCON WAIVER PROCESS</u></b></p> <ul style="list-style-type: none"> <li>• Have waivers been processed in writing for FPCON measures that are not being implemented?</li> <li>• Is the waiver process IAW the HHQ guidance?</li> <li>• Are compensatory measures developed for FPCON measures that have approved waivers? [Coordinate with all assessment team members.]</li> <li>• Is a process established to annually review waivers?</li> </ul>	<p>CJCSI 3121.01A DODD5210. 56</p> <p>Strategic Goal 2D</p>
SO-PLN-03	<p><b>Site-specific FPCON Measures.</b> Installation commanders shall develop and implement site-specific FPCON measures for stationary and in-transit forces to supplement the FPCON measures and actions enumerated for each FPCON level in enclosure 4 of DODI 2000.16.</p> <ul style="list-style-type: none"> <li>• Has the installation developed site-specific FPCON measures?</li> <li>• Do site-specific FPCON measures include the DOD minimum that must be implemented when a change in local threat warrants a change in FPCON or when higher authority directs an increase in FPCON?</li> <li>• Are site-specific FPCON measures also developed for in-transit forces?</li> <li>• Are the site-specific FPCON measures appropriately classified?</li> <li>• Do the development of site-specific FPCON measures permit sufficient time and space to determine hostile intent, while fully considering constraints imposed by the Standing Rules of Engagement (CJCSI 3121.01A) and Rules of Force (DOD Directive 5210.56)?</li> <li>• Are organic intelligence, counterintelligence, and law enforcement resources; institutional knowledge of the area of AT responsibility; and comprehensive understanding of organic capabilities, supported by national and AOR assets, leveraged in directing tailored FPCON measures for specific sites for stationary and in-transit forces?</li> </ul>	<p>DOD Std 22</p> <p>DOD 0- 2000.12-H Chapter 10</p> <p>CJCSI 3121.01A DODD 5210. 56</p> <p>Strategic Goal 2D</p>

**FOR OFFICIAL USE ONLY**

	<b>RANDOM ANTITERRORISM MEASURES (RAM)</b>	
SO-PLN-04	<p><b>Random Antiterrorism Measures (RAM).</b> The Installation Commander shall develop and implement RAM as an integral component of the overall AT Program.</p> <p><b><u>RAM PROCESS</u></b></p> <ul style="list-style-type: none"> <li>• Does the RAM program comply with HHQ guidance?</li> <li>• Does the RAM program change the installation’s AT tactics, techniques, and procedures so that they ensure a robust security posture?</li> <li>• Is the program unpredictable and ambiguous to instill uncertainty in terrorist planning?</li> <li>• Are RAMs used throughout all FPCON levels?</li> </ul> <p><b><u>RAM DEVELOPMENT / IMPLEMENTATION</u></b></p> <ul style="list-style-type: none"> <li>• Has the installation assessed local threat capabilities and identified effective RAM countermeasures to mitigate installation vulnerabilities?</li> <li>• Are RAMs selected from higher FPCONs as well as other measures not normally associated with FPCONs (Command-developed measures or locally developed, site-specific measures)?</li> <li>• Are RAMs conducted both internally to the installation and externally in coordination with local authorities?</li> </ul> <p><b><u>RAM MANAGEMENT</u></b></p> <ul style="list-style-type: none"> <li>• Has the Commander designated an office of responsibility for the RAM program?</li> <li>• Is the RAM program coordinated with Security Forces regarding RAM measures that require security personnel?</li> <li>• Does the office of responsibility monitor, track, and analyze RAM implementation efforts of all units?</li> <li>• Are spot checks conducted to determine if RAMs are being conducted?</li> </ul> <p><b><u>UNIT/TENANT INVOLVEMENT</u></b></p> <ul style="list-style-type: none"> <li>• Do all assigned and tenant units / agencies / activities support the RAM program?</li> <li>• Are assigned units and tenants allowed to develop / implement their own RAMs?</li> <li>• Are tenant conducted RAMs tracked?</li> </ul>	<p>DOD Std 14</p> <p>DOD 0-2000.12-H, Chapter 10</p> <p>Strategic Goal 2D</p>

## FOR OFFICIAL USE ONLY

<b>AT PHYSICAL SECURITY MEASURES</b>		
SO-PLN-05	<p><b>AT Physical Security Measures.</b> Installation commanders shall apply the principles of the Physical Security Program and fully integrate them into AT Plans to ensure employment of a holistic security system to counter terrorist capabilities.</p> <ul style="list-style-type: none"> <li>• Does the Physical Security Program integrate and synchronize the following with the AT Program:                             <ul style="list-style-type: none"> <li>○ Detection (human, animal, or sensors to alert security personnel of possible threats and unauthorized entry attempts at or shortly after occurrence)?</li> <li>○ Assessment (electronic audio-visual means, security patrols, or fixed posts to localize and determine the size and intentions of unauthorized intrusions or activity)?</li> <li>○ Delay/denial (active and passive security measures, including barriers, to impede intruders efforts)?</li> <li>○ Communication (command and control procedures)?</li> <li>○ Response (trained and properly equipped security forces)?</li> </ul> </li> <li>• Is the physical security program based on the threat and criticality assessment?</li> <li>• Does the installation have a Physical Security Plan?</li> <li>• Do measures include the development of access control procedures for ingress and egress control?</li> <li>• Is CBRN protection included in the Physical Security Program, to include the postal system?</li> <li>• Is barrier planning and stand-off included in the program? [Coordinate with Security Engineering.]</li> </ul>	<p>DOD Std 13</p> <p>DOD 5200.8-R</p> <p>DOD 0-2000.12-H Chapter 22</p>
<b>SECURITY FORCES</b>		
SO-PLN-06	<p><b>Security Force Operations.</b> The installation's Physical Security Program shall include the integration of security forces for detection, assessment, and response.</p> <ul style="list-style-type: none"> <li>• Is there an identified immediate response force?</li> <li>• Is the response force capable of slowing the advance of the aggressors?                             <ul style="list-style-type: none"> <li>○ Facilitate the evacuation of the protected asset to safe areas.</li> <li>○ Secure the protected asset and contain the threat.</li> <li>○ Prevent additional hostile resources from arriving and prepare to apprehend the threat and relieve the protected asset.</li> </ul> </li> <li>• Does the security force's operation planning address the following:                             <ul style="list-style-type: none"> <li>○ Organization, training, and equipping of augmentation security forces?</li> <li>○ Primary and alternate dispatch location?</li> <li>○ Primary and alternate arming point?</li> <li>○ Pre-planned response for threats (at a minimum those identified in the threat assessment)?</li> <li>○ Overt attack?</li> <li>○ Protection of Distinguished Visitors/HRPs?</li> <li>○ Prioritized posting for FPCONs?</li> <li>○ Contingency Operations?</li> </ul> </li> <li>• Does the installation have enough security forces (include augmentees) to man the installation through FPCON DELTA?</li> </ul>	<p>DOD Std 13</p> <p>DOD O-2000-12-H, Chapter 22</p>

**FOR OFFICIAL USE ONLY**

	<p><b><u>REACTION FORCE TRAINING</u></b></p> <ul style="list-style-type: none"> <li>• Has the reaction force been formed, equipped (including CBRNE equipment), and mission-specific trained (e.g., building entry and search techniques, vehicle assault operations, anti-sniper techniques, equipment)?</li> <li>• Has the force been briefed on the laws and policies governing the use of force and the use of deadly force in the protection of DOD personnel, facilities, and materiel?</li> <li>• Has the force been trained and exercised under realistic conditions?</li> <li>• Has the reaction force been tested quarterly (alert procedures, response time, overall preparedness)?</li> <li>• Has a hostage negotiations team been identified? Has the negotiation team been trained and exercised under realistic conditions?</li> <li>• Does plan include the potential for an interpreter?</li> </ul>	
SO-PLN-07	<p><b>Security Forces Arming.</b> DOD personnel regularly engaged in law enforcement or security duties shall be armed.</p> <p><b><u>ARMED</u></b></p> <ul style="list-style-type: none"> <li>• Are all personnel who regularly perform law enforcement or security duties armed?</li> <li>• Are personnel authorized to carry firearms qualified with their applicable weapon(s)?             <ul style="list-style-type: none"> <li>○ Have all personnel issued firearms qualified at least annually?</li> <li>○ Are records of individual qualification results retained for as long as the individual possesses a firearm?</li> </ul> </li> <li>• Was the decision to arm or not arm based on a reasonable expectation that life or DOD assets will be jeopardized if firearms are not carried?</li> </ul> <p><b><u>UNARMED</u></b></p> <ul style="list-style-type: none"> <li>• Was evaluation of the necessity to carry a firearm made considering this expectation weighed against the possible consequences of accidental or indiscriminate use of firearms?</li> <li>• Did the local Commander evaluate the probability of the threat in a particular location, the adequacy of support by DOD protective personnel, the adequacy of protection by U.S. or host-nation authorities, and the effectiveness of other means to avoid personal attacks?</li> <li>• Have all armed personnel undergone a background check to ensure no conditions exist that would prohibit the individual from being armed?</li> </ul>	<p>DOD Std 13</p> <p>DODD 5210.56, Para 4.1 Enclosure 1, Para E1.1.4</p>

**FOR OFFICIAL USE ONLY**

	<p><b><u>USE OF FORCE</u></b></p> <ul style="list-style-type: none"> <li>• Has the local Commander developed use of force guidance based on DOD Directive or Service directive?</li> <li>• Has the General Counsel/Staff Judge Advocate (SJA) reviewed and approved the local use of force rules?</li> <li>• Have all armed personnel been trained on the local use of force rules?             <ul style="list-style-type: none"> <li>○ Are personnel who have not received use of force training prohibited from carrying firearms?</li> </ul> </li> <li>• Is annual refresher training given to all personnel assigned to law enforcement and security duties to ensure that they continue to be thoroughly familiar with all restrictions on the use of deadly force?</li> <li>• Is there a nonlethal use of force option available for use?</li> <li>• If posted personnel are carrying their civilian law enforcement agency issued nonlethal equipment, has the installation SJA coordinated/approved its use? (Guard /Reserve Bases.)</li> </ul> <p><b><u>CONTRACT SECURITY</u></b></p> <ul style="list-style-type: none"> <li>• Has the local Commander developed criteria for the carrying of firearms by contract security forces?</li> <li>• Has the rules of engagement and/or use of force policy been developed for contract security forces?</li> </ul>	<p>DODD 5210.56, Enclosure 2, Para E2.1.4</p> <p>DODD 5210.56, para 5.3.3</p>
SO-PLN-08	<p><b>Security Force Training.</b> The installation’s Physical Security Program shall include trained Security Forces capable of performing detection, assessment, delay, and response.</p> <ul style="list-style-type: none"> <li>• Is there a formal training/certification program for installation security forces and augmentors?</li> <li>• Does the training program consist of initial and recurring type training?</li> <li>• Does the training consist of the following areas:             <ul style="list-style-type: none"> <li>○ Access control procedures?</li> <li>○ Operation of security equipment (e.g., barriers, explosive detection equipment)?</li> <li>○ Training/qualification with assigned weapons?</li> <li>○ Force-on-force training?</li> <li>○ Antiterrorism-related training?</li> <li>○ Response to critical assets and contingencies?</li> </ul> </li> <li>• Are all Security Force personnel performing access control procedures trained on the operation of the barrier system?</li> <li>• Have vehicle inspection instructions been developed?</li> <li>• Have security forces and augmentors received adequate vehicle search training?</li> <li>• Do security forces receive training on improvised explosive devices? (preferably by EOD)?</li> <li>• Is there a process to exercise the use of augmentees to verify availability and serve as a RAM?</li> <li>• Have security forces been trained on surveillance detection?</li> <li>• Do security forces receive training on current terrorist tactics, techniques, and procedures?</li> </ul>	<p>DOD Std 13</p> <p>DOD O-200012-H, Chapter 22</p>

**FOR OFFICIAL USE ONLY**

	<p><b><u>TRAINING FOR CONTRACT SECURITY GUARDS</u></b></p> <ul style="list-style-type: none"> <li>• Does the contract stipulate training requirements?</li> <li>• Have the contract guards been trained IAW the task outlined in their contact?</li> <li>• Is training provided on security equipment purchased by the military installation?</li> <li>• Does the contract officer technical representative or his/her designee monitor the training of contract security guards?</li> <li>• Do contract guards engage in joint training with the assigned military security force?</li> </ul>	
SO-PLN-09	<p><b>Security Forces Equipment.</b> Installation Security Forces shall be equipped to accomplish the mission of protecting DOD assets on the installation.</p> <ul style="list-style-type: none"> <li>• Are Security Forces personnel equipped with appropriate weaponry as identified in the AT Plan and operating instructions?</li> <li>• Is the quantity / type of weapons on-hand sufficient to equip Security Forces and augmentees through FPCON DELTA?</li> <li>• Are Security Forces equipped with individual protective equipment to respond to a CBRNE event?</li> <li>• Do Security Forces have ballistic protection and is it worn as required?</li> <li>• Are Security Force augmenters similarly equipped as the Security Forces?</li> <li>• Do Security Forces have explosive detection equipment for use at access control points, special events, and facilities?</li> </ul> <p><b><u>MILITARY WORKING DOG PROGRAM</u></b></p> <ul style="list-style-type: none"> <li>• Do the security forces have explosive detection dogs to complement the vehicle search and RAM programs?</li> <li>• Is there a certification process for explosive detection dogs?</li> <li>• If contract dogs are used, did the installation observe / mandate the certification process for the explosive detection dogs? (Determine the detection capabilities and type and probability of detection.)</li> <li>• Are MWDs used on a recurring basis to enhance detection and deterrence? (Drug and patrol dogs can be used at ACPs for deterrence.)</li> <li>• Are MWDs integrated into the IDS (e.g. patrolling critical facilities, checking parking lots, patrolling perimeter)?</li> <li>• Do security forces use MWDs to conduct sweeps of exterior/interior areas of observation and concealment points, and does this area extend as far out as 1,000 meters from the protected resource?</li> <li>• Are MWDs used on response elements to enhance internal and external intruder detection capabilities?</li> </ul>	<p>DOD Std 13</p> <p>DOD O-200012-H, Chapter 22</p>

## FOR OFFICIAL USE ONLY

### VEHICLES

- Are appropriate type of vehicles assigned based upon topography, intended use (i.e., escort, area patrol, off road), and response?
- Are armored vehicle available, if required?
- Are vehicles properly marked as response vehicles if not used for covert operations?
- Are vehicles appropriately equipped:
  - Emergency lights and sirens?
  - Public address systems?
  - Search lights?
  - Emergency road kit?
  - First aid kit?
  - Bio-hazard kit?
  - Radios?
  - Installation map?
  - Post orders?

### COMMUNICATIONS

- Is the Security Force's radio net equipped with a minimum of two frequencies?
- Is the Security Force's radio net provided with secure voice capabilities or compliant with Data Encryption Standards (DES)? [Coordinate with Emergency Management.]
- Are the land mobile radios, base stations, and repeaters equipped with uninterrupted power supplies?
- Are radios interoperable with other first responders, including host-nation and local authorities? If not, are there procedures in place to mitigate this gap? [Coordinate with Emergency Management.]
- Is each static post provided a portable or fixed two-way radio or phone?
- Are mobile patrols provided a minimum of one portable radio?
- Is there a radio prioritization for expanded security operations?
- Is there an alternate means of communications for Security Forces?
- Is there a duress system (vocal or mechanical) built into the communications system?

### EQUIPMENT FOR CONTRACT SECURITY GUARDS

- Are contract guards equipped IAW their contract?
- Do contract guards have radios compatible with the assigned military force and/or can they communicate with responding local / host-government forces?
- Do contract guards have OSHA-approved individual protective gear?
- Are contract guards incorporated into the installation's duress program?

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

	<p><b><u>DURESS PROGRAM</u></b></p> <ul style="list-style-type: none"> <li>• Is there a process to change the duress code when compromised or at least every six months?</li> <li>• Are duress codes protected as “FOR OFFICIAL USE ONLY” or higher?</li> <li>• Is there a duress code for facilities and is this code known by appropriate Security Forces (e.g., alarm monitor, responding patrols)?</li> <li>• Is there a duress code for high-risk personnel and PSDs and is this code known by entry controllers and other key Security Force members?</li> <li>• Are duress alarms positioned so that they can be activated without arousing suspicion?</li> <li>• Are duress alarms at security post tested a minimum of daily?</li> <li>• Do owner users test their own duress alarms at least quarterly?</li> <li>• Are response procedures developed for duress activation?</li> </ul> <p><b><u>ALTERNATE ARMING POINT</u></b></p> <ul style="list-style-type: none"> <li>• Is there an alternate arming point for the Security Forces?</li> <li>• Is the alternate arming point exercised?</li> <li>• Is the alternate arming point out of the potential danger area posed at the main armory?</li> <li>• Are sufficient weapons stored for responding forces?</li> <li>• Is there a process to access the alternate armory during non-duty hours?</li> <li>• Are there written procedures for activating the alternate armory?</li> </ul>	
<b>INSTALLATION ACCESS CONTROL</b>		
SO-PLN-10	<p><b>Access Control Procedures.</b> DOD installations shall establish access control points (ACP) to ensure the proper level of access control for all DOD personnel, visitors, and commercial traffic to an installation. The objective of an ACP is to secure the installation from unauthorized access and intercept contraband (weapons, explosives, drugs, classified material, etc.) while maximizing vehicular traffic flow.</p> <ul style="list-style-type: none"> <li>• Are access control procedures developed around the design basis threat?</li> <li>• Has the installation developed written access control procedures for each FPCON? <ul style="list-style-type: none"> <li>○ Describes specific missions of the post</li> <li>○ Addresses acceptable identification types</li> <li>○ Describes emergency entry procedures</li> <li>○ Current and covers changes that have been implemented [access control process, etc.]</li> <li>○ Covers operation of barriers at the post</li> <li>○ Contains gate procedures for alarm situations</li> <li>○ Covers barment of personnel</li> <li>○ Addresses vehicle, pedestrian, and commercial deliveries</li> </ul> </li> <li>• Do procedures define who can enter the installation and the required identification?</li> <li>• Do access control procedures reduce access as the FPCON level increases?</li> <li>• Are access control measures commensurate with current HHQ guidance, i.e. searching commercial deliveries?</li> <li>• Are entry access lists required to be authenticated before being accepted by the entry controller?</li> <li>• Have personnel designated with escort privileges been trained on their duties</li> </ul>	

## FOR OFFICIAL USE ONLY

	<p>and is there a maximum number of personnel an escort can escort? [Applies to facilities as well.]</p> <ul style="list-style-type: none"><li>• Is there a formal process to vouch personnel onto the installation?</li></ul> <p><b><u>ACP OPERATIONS</u></b></p> <ul style="list-style-type: none"><li>• Is the ACP capable of accommodating random antiterrorism measures (RAMs)?</li><li>• Have gates been designated for operation during all FPCONs?</li><li>• Are designated gates capable of performing 100% vehicle inspections?</li><li>• Has a commercial gate been designated for all commercial deliveries?</li><li>• Is each ACP equipped with at least two means of communications to the security control center? Consider emergency ring down.</li><li>• Is the ACP capable of connecting to the installation's intranet? (Should be password protected and properly shut down when gate is closed; consider a removable hard drive.) [Not required, but increases efficiency.]</li><li>• Is each ACP equipped with a duress alarm that annunciates at the security control center? (Activation of the emergency barrier operation could be configured to activate the duress alarm.)</li></ul> <p><b><u>ACP OVERWATCH</u></b> May not be applicable at all installations. Must have a clear field of fire past the installation ACP.</p> <ul style="list-style-type: none"><li>• Has the installation included overwatch positions in their FPCON planning?</li><li>• Have rules of engagement been developed for the overwatch position?</li><li>• Have detailed standard operating procedures been developed that include command and control between the overwatch and the ACP?</li></ul> <p><b><u>VEHICLE SEARCHES</u></b></p> <ul style="list-style-type: none"><li>• Is a commercial vehicle search area established?</li><li>• Are procedures for conducting vehicle searches established?</li><li>• Are Security Forces trained on conducting vehicle searches?</li><li>• Is sustainment training developed?</li><li>• Are explosive detection dogs or mechanical explosive detection equipment used?</li><li>• Have standard operating procedures for use of explosive detection equipment developed?</li><li>• Are drivers asked to exit vehicles?</li><li>• Are vehicle searches concealed from observation?</li></ul>	
--	---	--

## FOR OFFICIAL USE ONLY

O-PLN-11	<p><b>Perimeter Security.</b> The installation shall develop a barrier system that establishes a perimeter to establish boundaries and deter/intimidate individuals from attempting unlawful or unauthorized entry.</p> <ul style="list-style-type: none"><li>• Has the installation established a perimeter protection system?</li><li>• Is there an active perimeter inspection/maintenance program on the installation?</li><li>• Is an unobstructed area or clear zone [recommend 30 feet on both sides for trees etc.; refer to UFC for facilities] maintained on both sides of the permanent physical barriers?</li><li>• Are dips, ridges, ditches, etc., or other concealment areas removed from the clear zone?</li><li>• Is there an Intrusion Detection System (IDS) on the exterior perimeter to provide the earliest possible notification and identification of an intrusion? (Based on the level of protection required for the asset.)</li><li>• Are walls that form the perimeter boundary topped with barbed wire?</li></ul> <p><b><u>FENCING</u></b></p> <ul style="list-style-type: none"><li>• Is the fence a height of seven feet without outriggers and eight feet with outriggers?</li><li>• Is the perimeter fence topped with concertina wire and/or outriggers (two 15-inch Y outriggers having three strands of barbwire each)?</li><li>• Are posts, bracing, and other structure members on the inside (site side) of the fence fabric?</li><li>• Is the fence fabric secured to tension wires with 12-gauge galvanized tie wire?</li><li>• Is the fence fabric secured to fence posts, rails, or other anchoring material with fasteners of tensile strength at least equal to the fence fabric?</li><li>• Is the bottom of the fence fabric within 2 inches of firm ground or buried in other soils? Curbs, sills, etc., can be used to fill in gaps.</li><li>• Is the perimeter fence reinforced through installation of vertical support posts installed at 4-foot intervals or arresting cables installed parallel to the ground at 6 inches and then 30 inches above the ground? [Coordinate with Structural Engineer.]</li><li>• Are installation warning signs posted not to exceed 100 yards apart?</li></ul> <p><b><u>UNMANNED GATES</u></b> [Coordinate with Structural Engineer]</p> <ul style="list-style-type: none"><li>• Are gates that are not in regular use secured? [Can't be rammed open or opened by hand.]</li><li>• Are the bottom of the gates within five inches of pavement and 2 inches for soil?</li><li>• Are there no more than five inches between the gate and gatepost?</li><li>• Are gates secured with Type II or III Secondary padlock if not equipped with electric locks?</li><li>• Are keys to perimeter gates restricted to the Security Forces?</li><li>• Are gates checked each shift and does this include verifying that the lock in use belongs (unlock and relock, rotate locks, number locks) to the Security Forces and not some other activity or would-be intruder?</li></ul>	DOD Std 13  DOD O-2000.12-H, Chapter 23
----------	---	---

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

<b>ELECTRONIC SECURITY SYSTEM (ESS)</b>		
<p><b>SSO-PLN-12</b></p>	<p><b>Electronic Security System (ESS).</b> The installation Physical Security Program shall include a security system capable of protecting DOD Assets.</p> <ul style="list-style-type: none"> <li>• Does the physical security system perform the following functions:               <ul style="list-style-type: none"> <li>○ Threat Detection?</li> <li>○ Threat Annunciation?</li> <li>○ Threat Classification and Assessment?</li> <li>○ Threat Delay?</li> </ul> </li> </ul> <p><b><u>THREAT DETECTION</u></b> The threat detection system should provide as early as possible detection to increase the opportunities to protect DOD assets and minimize the impact of terrorist acts against DOD personnel, materiel, and facilities.</p> <ul style="list-style-type: none"> <li>• Were the following considerations used to determine the appropriate surveillance systems performance and selection:               <ul style="list-style-type: none"> <li>○ Seasonal and/or ambient weather conditions?</li> <li>○ The type of background against which surveillance systems are attempting to operate? (Can affect sensitivity.)</li> <li>○ Environmental and/or geographical considerations regarding where the systems are placed, making use of key terrain (hills, ditches, roads) or on fixed, man-made barriers (fences, walls, barriers)?</li> </ul> </li> <li>• Does the installed alarm sensor system perform the following functions:               <ul style="list-style-type: none"> <li>○ Line of detection on a fence:                   <ul style="list-style-type: none"> <li>▪ Detect cutting?</li> <li>▪ Detect climbing on the fence?</li> <li>▪ Detect lifting the fence?</li> </ul> </li> <li>○ Line of detection at the area perimeter, in a clear zone, airfield taxi gap, or around individual resources?</li> <li>○ Detect walking:                   <ul style="list-style-type: none"> <li>▪ Detect running?</li> <li>▪ Detect rolling?</li> <li>▪ Detect crawling across?</li> <li>▪ Detect jumping through the line of detection?</li> </ul> </li> <li>○ Line of detection at a facility?                   <ul style="list-style-type: none"> <li>▪ Must detect intrusion attempts through likely avenues:                       <ul style="list-style-type: none"> <li>• Intrusion through doors.</li> <li>• Intrusion through windows.</li> <li>• Intrusion through walls.</li> <li>• Instruction through roof or vents.</li> </ul> </li> </ul> </li> </ul> </li> </ul>	<p>DOD Std 13</p> <p>DOD O- 2000.12-H, Chapter 22</p>

## FOR OFFICIAL USE ONLY

SO-PLN-12A	<p><b><u>THREAT ANNUNCIATION</u></b> The threat detected by the security system must be reported to a central location where Security Forces can be dispatched.</p> <p><b><u>CONSTRUCTION OF THE CONTROL CENTER</u></b></p> <ul style="list-style-type: none"><li>• Is the system located in a restricted area and closed off from public view?</li><li>• Is the facility constructed with suitable ventilation, heating, and air conditioning?</li><li>• Is the facility equipped with doors that lock when not in use and a cipher lock or Automated Entry Control System (AECS) on the main entry door?</li><li>• Is there one-way glass panel, CCTV coverage, or similar viewing device to identify personnel requesting entry?</li><li>• Is the main terminal for the Land Mobile Radio (LMR) base station and landline system installed in the control center?</li><li>• Is the control center equipped with landline communications to each fixed, permanent, and static access control post, command post, control tower, fire department, subordinate C3 facility, flight line maintenance, and munitions control, as applicable?</li></ul> <p><b><u>ALARM MONITORING STATION</u></b></p> <ul style="list-style-type: none"><li>• Is there an annunciation capability where Security Forces can be immediately dispatched?</li><li>• Are alarms audible and visual?</li><li>• Are all alarms recorded?</li><li>• How are systems malfunctions recorded and reported?</li><li>• Has a nuisance rate been established for the system? What is the nuisance rate (e.g., per 24-hour per sensor field, etc.)?</li><li>• Has the installation command structure determined what constitutes catastrophic, major, and partial failure of the IDS?<ul style="list-style-type: none"><li>○ Are there contingency plans / compensatory measures for each type of failure?</li></ul></li><li>• Has a maintenance response priority been established for each type of failure?</li><li>• Is there a redundant capability for this system?</li><li>• Are the data transmission lines secured?</li></ul>	DOD Std 13  DOD O-2000.12-H, Chapter 22.5.5
------------	--	---

## FOR OFFICIAL USE ONLY

<p>SO-PLN-12B</p>	<p><b><u>THREAT CLASSIFICATION AND ASSESSMENT</u></b> - The physical security system should be able to determine whether the alarm is real or false and if the intrusion is hostile or benign.</p> <ul style="list-style-type: none"> <li>• Is a CCTV system employed to assist in the alarm assessment role?</li> <li>• Is the CCTV system connected as a slave to the IDS? (Video interfaced for alarm assessment camera call-up)</li> <li>• Does the security system include a night viewing device, an imaging infrared device, human intervention, or other method of assist in classifying the threat?</li> <li>• Is there a video recording capability for forensics? (Digital is preferred.)</li> <li>• Is lighting adequate to assess the threat? (6 to 1 Light to Dark Ratio.)</li> <li>• Is CCTV coverage provided for the following interior areas: <ul style="list-style-type: none"> <li>○ Card reader door assessment.</li> <li>○ Emergency exit door assessment.</li> <li>○ Surveillance of lobbies, entrances, corridors, and open areas.</li> <li>○ Is fiber optic (preferred type) used as the transmission system from the CCTV to the central-monitoring station?</li> </ul> </li> </ul> <p><b><u>THREAT DELAY</u></b> The physical security system should have a built in delay system that provides the minimum delay time on any path to the protected area.</p> <ul style="list-style-type: none"> <li>• Has the minimum delay time been established? (Note: measures from the time the intruder is detected until the intruder has penetrated all of the barriers, including the time it takes to travel from barrier to barrier, and the protected area.)</li> <li>• Is perimeter, exterior, and interior physical barriers (erected or installed) (fences, gates, walls, windows, doors, locking systems, ceilings, and floors) incorporated into the delay system?</li> <li>• Does the delay system meet the minimum delay requirement established by the installation?</li> <li>• Does the delay system meet the three requirements for a delay system: <ul style="list-style-type: none"> <li>○ Facilitate definitive threat classification and assessment?</li> <li>○ Facilitate response by Security Forces?</li> <li>○ Facilitate evacuation of protected DOD assets if evacuation is the most appropriate, cost-effective AT remedy?</li> </ul> </li> </ul>	<p>DOD Std 13</p> <p>DOD O-2000.12-H, Chapter 22.4.3</p>
<p>SO-PLN-13</p>	<p><b><u>Installation Lighting.</u></b> The installation lighting system should enable Security Forces to observe activities around or inside an installation without disclosing their presence.</p> <ul style="list-style-type: none"> <li>• Does the installation lighting provide Security Forces with the capability to see low contrasts, such as indistinct outlines or silhouettes, and spot intruders who may be only exposed for a few seconds?</li> <li>• Does the level of lighting take into consideration the contrast between the intruder and the background?</li> <li>• Are controls for security lighting secured inside the protected area and locked or guarded at all times? (Note: High-impact plastic shields may be installed over lights to prevent destruction by stones or air rifles.)</li> </ul>	<p>DOD Std 13</p> <p>DOD O-2000.12-H, Chapter 22.6</p>

## FOR OFFICIAL USE ONLY

SO-PLN-14	<p><b>Bomb Threat Plans.</b> The installation shall develop plans/procedures to respond to a bomb threat.</p> <ul style="list-style-type: none"> <li>• Has the installation developed a bomb threat response plan?</li> <li>• Does the installation bomb threat response plan include the following processes: <ul style="list-style-type: none"> <li>○ Bomb threat mitigation?</li> <li>○ Notification and evacuation procedures?</li> <li>○ Search procedures?</li> </ul> </li> <li>• Does the installation AT Plan identify requirements for facility-specific bomb threat plans (i.e., a template)?</li> <li>• Has the bomb threat response plan been reviewed by EOD?</li> <li>• What is the response time for EOD to arrive? (Coordinate with EM.)</li> <li>• If no organic EOD capabilities exist, are there agreements to get the support from the local / host-government authorities?</li> <li>• What are the interim measures that are implemented until arrival of EOD?</li> <li>• Are bomb threat plans included in AT Review and Exercise Programs?</li> </ul>	DOD Std 7
-----------	--	-----------

### MAIL HANDLING PROCEDURES

SO-PLN-15	<p><b>Mail Handling Procedures.</b> Installations shall develop preventative measures against the introduction of explosives and chemical or biological-laden mail from entering the installation's mail handling system.</p> <ul style="list-style-type: none"> <li>• Has the installation conducted an assessment of its mail system to determine if mail screening is accomplished at any point in the delivery process? [Explosives as well as chemical/biological contaminants.]</li> <li>• If mail is screened, is there a process to verify integrity of the mail from point of inspection to delivery?</li> <li>• If mail is not screened, has the installation developed a process and procured required equipment to perform screening?</li> <li>• Has the installation / facility developed formal, site-specific procedures for explosives and chemical/biological suspicious mail? [Separate and distinct procedures.]</li> <li>• Are all personnel who handle mail trained on these procedures?</li> <li>• Are training aids available in the mail room?</li> <li>• Are mail handlers trained on the mail screening devices?</li> <li>• Is there a process to conduct routine testing of the mail screening devices, i.e., sending through a simulated threat?</li> <li>• Is the mail room equipped with the following equipment for chemical / biological incidents: <ul style="list-style-type: none"> <li>○ Gloves (avoid powder-coated gloves)?</li> <li>○ Large sealable bags for isolating suspicious mail and discarding all clothing worn during contact with contaminants?</li> <li>○ Change of clothing?</li> <li>○ Surgical mask or protective mask? (Commercial mask are available.)</li> </ul> </li> <li>• Are mail handlers informed and trained on how to shut down the ventilation system in case of airborne contaminants?</li> <li>• Is the mail handling plan exercised? [coordinate with the Infrastructure Engineer]</li> <li>• Are there plans for a central mail delivery / inspection center during increased FPCON?</li> </ul>	DOD Std 13  DOD O-2000.12-H, AP3, Tab C
-----------	---	---

**FOR OFFICIAL USE ONLY**

<b>AT MEASURES FOR HIGH-RISK PERSONNEL (HRP)</b>		
SO-PLN-16	<p><b>High-Risk Personnel.</b> Installation commanders shall develop AT measures for personnel designated high-risk personnel (HRP), for those personnel occupying High-Risk billets (HRB), and for other senior executive personnel designated as distinguished visitors.</p> <ul style="list-style-type: none"> <li>• Are there any officially (through Military Service channels) designated HRP or HRB assigned to the installation?</li> <li>• Is a process to conduct a PSVA on HRPs established?</li> <li>• Is there a process to initiate PSVA within 90 days of an individual's assignment to a HRB?</li> <li>• Are PSVAs revalidated annually and updated if the Terrorism Threat Level changes or at least every three years?</li> <li>• Has the installation developed protective measures for HRPs?</li> <li>• Are the protective measures promulgated in the AT Plan?</li> <li>• Are protective measures tied to the FPCON system?</li> </ul> <p><b><u>HRP/HRB TRAINING</u></b></p> <ul style="list-style-type: none"> <li>• Has the installation established required training for HRP/HRB?</li> <li>• Does training include familiarization with treaty, statutory, policy, regulatory, and local constraints on the application of supplemental security measures for certain high-ranking DOD officials who are entitled to additional measures as a result of their position. [OCONUS]</li> <li>• Is there a process to notify Military Services of personnel and their family members requiring formal HRP training before assignment?</li> <li>• Is there a process to ensure HRP and family members, as appropriate, complete the required high-risk training (personal protection, evasive driving, terrorism awareness, and hostage survival)?</li> </ul>	<p>DOD Std 16</p> <p>Strategic Goal 3D</p> <p>DODI 2000.22</p>

## FOR OFFICIAL USE ONLY

SO-PLN-17	<p><b>Office Security.</b> The office environment for high-risk personnel should normally provide the greatest degree of protection. AT measures, guards, security checkpoints, office workers, aides, and/or secretaries all serve to insulate the designee from potential threats.</p> <ul style="list-style-type: none"> <li>• Has a vulnerability assessment of the office area been performed?</li> <li>• Are the following security enhancements selectively implemented in the office of HRPs and senior executives:             <ul style="list-style-type: none"> <li>○ Installation of surveillance systems?</li> <li>○ Access points away from the office entrance?</li> <li>○ Duress systems within the office?</li> </ul> </li> <li>• Install vehicle barriers and realign roadways to eliminate straight, level stretches of road in excess of 50 meters in length.</li> <li>• Increase concentric rings of fences, Jersey barricades, planters, bollards, and vehicle and/or personnel barriers.</li> <li>• Access control areas, supplemented by fire doors and/or security doors kept in the closed condition, between the entrance to the building housing executives offices and executive office area itself.</li> <li>• Confuse, camouflage, and deceive observers by hiding designee's location.</li> <li>• Consider relocating executives to buildings not usually associated with office activities, e.g. barracks, motor pool, and R&amp;D facilities. (Note: this may be included as an FPCON measure.)</li> <li>• Add executive style, decorative lighting, and window treatment to several different office buildings to minimize differences in external appearances.</li> <li>• Replace standard doors and door frames leading into the protected office with high security doors and doorframes.</li> <li>• Strengthen walls, floors, and ceilings against IED, small arms, incendiary devices, and powered hand tools by substituting steel plate, concrete filled, steel reinforced cinder blocks, or other ballistic-resistant materials.</li> <li>• Limit public available information, i.e. official biographies, to the bare minimum.</li> </ul> <p><b><u>SAFE HAVEN</u></b> Personnel requiring a high level of protection in high threat areas should include a <u>safe haven</u>. The safe haven should be the inner most layer of protection within a physical security system.</p> <ul style="list-style-type: none"> <li>• Was the safe haven designed to provide a minimum of 15 minutes of protection against a predetermined level of attack using hand tools or small arms?</li> <li>• Was the response time by the security force factored into the required delay?</li> <li>• Is the safe haven large enough to accommodate the personnel intended to use the location?</li> <li>• Is it free of windows and vents that could allow introduction of contaminants?</li> <li>• Is the safe haven equipped at a minimum with the following items:             <ul style="list-style-type: none"> <li>○ Food?</li> <li>○ Water?</li> <li>○ Medical supplies?</li> <li>○ Communications?</li> </ul> </li> </ul>	<p>DOD Std 16</p> <p>DODI 2000.22</p> <p>DOD O- 2000.12-H, Chapter 21</p>
-----------	---	---

## FOR OFFICIAL USE ONLY

SO-PLN-18	<p><b>Office Security Procedures.</b> Installations should implement special considerations for secretaries and executive assistants who also perform collateral security duties for high-risk personnel.</p> <ul style="list-style-type: none"> <li>• Are the following security considerations provided for the secretary and executive assistant: <ul style="list-style-type: none"> <li>○ Installation of physical barriers such as electromagnetically operated doors to separate offices of the high-risk personnel or senior executive from other offices?</li> <li>○ Installation of a silent duress alarm button with a signal terminating at the security department?</li> <li>○ Prevention of visitors from entering the protected area before being positively screened or through personal recognition? (Note: assumes secretaries and executive assistants are advised of employee threats or known acquaintances.)</li> <li>○ Prohibition on issuing information to unknown callers?</li> <li>○ Storage of first aid kit and fire extinguisher in the office area?</li> <li>○ Posted procedures for handling threatening calls?</li> <li>○ Prohibitions on accepting packages from strangers?</li> <li>○ Mail handing procedures?</li> <li>○ Limited distribution and visibility of travel itineraries and schedules of senior officials?</li> </ul> </li> </ul>	<p>DOD Std 16</p> <p>DODI 2000.22</p> <p>DOD O- 2000.12-H, Chapter 21</p>
SO-PLN-19	<p><b>Protective Security Details (PSD).</b> Installations shall provide Protective Security Details (PSD) for high-risk personnel, authorized key senior military officers, DOD civilians, other U.S. Government officials or foreign dignitaries requiring personal protection.</p> <ul style="list-style-type: none"> <li>• Is the level of protection for the protected appropriate for the threat?</li> <li>• Do personnel assigned PSDs meet Service regulation requirements?</li> <li>• Are travel itineraries reviewed by the PSDs to ensure protection of routes and times?</li> <li>• Is there a formal selection process for PSD members?</li> <li>• Is there a training program for PSD members?</li> <li>• Has an operating instruction been developed for PSD operations?</li> <li>• Do PSD personnel conduct training for protected and family members on means to protect themselves, respond to an attack, and how to conduct themselves properly if captured? <ul style="list-style-type: none"> <li>○ Duress signals.</li> <li>○ Call-in.</li> <li>○ Carrying duress notes written on money.</li> <li>○ Duress alarms and/or radio links.</li> <li>○ Varying routes.</li> <li>○ Clothing changes.</li> <li>○ What to do if taken captive.</li> <li>○ Contact with police.</li> </ul> </li> <li>• Is PSD provided detailed information on the location of the safe havens, pre-surveyed evacuation sites, pre-surveyed evacuation routes, and identified back-up or alternatives?</li> </ul>	<p>DOD Std 16</p> <p>DODI 2000.22</p> <p>DOD O- 2000.12-H, Chapter 21, C21.10 and APP 15</p>

## FOR OFFICIAL USE ONLY

<b>AT MEASURES FOR LOGISTICS and CONTRACTING</b>		
SO-PLN-20	<p><b>Logistics and Contracting.</b> Installation commanders shall incorporate AT measures into the logistics and contracting process (requirements development, vendor selection, award, execution, and evaluation) when the provisions of the contract or services provided impact the security of DOD elements; personnel; or mission-essential cargo, equipment, assets, or services.</p> <ul style="list-style-type: none"> <li>• Has the installation developed AT measures for the contracting office to include in applicable contracts?</li> <li>• Is there a provision for the contracting office and the unit to notify the ATO of pending contracts?</li> <li>• Is there a process to ensure that contracts comply with the AT provisions in the Defense Federal Acquisition Regulation Supplement (DFARS)?</li> <li>• Is the ATO coordinating contracting requirements with the contracting officer and the legal office on contracts that affect the security posture?</li> <li>• Are contracting security requirements based on the individual threat concerns and arrangements with the host nation?</li> <li>• Are contracting procedures referenced or included in the AT Plan?</li> <li>• Is the Commander's guidance for the AT security criteria applied as a baseline for all contracts?</li> <li>• Are contracts/contractors included during the Commander's AT risk assessment process?</li> <li>• Is the contractor's performance evaluated when future contracts are awarded?</li> </ul>	<p>DOD Std 18</p> <p>DOD O-2000.12-H, AP8.1.1.</p> <p>Strategic Goal 2D</p>
SO-PLN-21	<p><b>Background Investigation for Contractors.</b> Installation commanders shall implement a verification process, whether through background checks or other similar processes, that enables the U.S. Government to attest to the trustworthiness of DOD contractors and sub-contractors (U.S. Citizens and host-nation personnel), including those personnel having direct or indirect involvement in the delivery or provision of services related to mail, supplies, food, water, or other material and equipment for use by DOD personnel.</p> <ul style="list-style-type: none"> <li>• Is there a process to conduct background or similar checks on contractors and sub-contractors?</li> <li>• Does the installation have a process to verify that background checks have been conducted?</li> <li>• Do background checks include husbanding agents and crews on contracted ships, planes, and overland vehicles?</li> <li>• Are contractor personnel screening requirements met before the start of the contract?</li> <li>• If screening is not completed, is there a process to escort personnel until screening is completed?</li> <li>• Is there a provision for the contracting office and the unit to notify the ATO prior to the contracting services starting so he or she can ensure all AT security measures are in place?</li> </ul>	DOD Std 18

**FOR OFFICIAL USE ONLY**

SO-PLN-22	<p><b>Site-specific Risk Mitigation.</b> The Installation Commander shall develop and implement site-specific risk mitigation measures to maintain positive control of DOD contractors and sub-contractors' access to and within the installation, sensitive facilities, and classified areas.</p> <ul style="list-style-type: none"> <li>• Are contractors provided security briefs on circulation control?</li> <li>• Have risk mitigation measures been developed for the installation?</li> <li>• Are contract security requirements incorporated into the local FPCON measures?</li> <li>• Are special security concerns listed in the contract security requirements?             <ul style="list-style-type: none"> <li>○ Frequent, random patrols.</li> <li>○ Inspections.</li> <li>○ Spot-checks.</li> <li>○ Food, water, and petroleum distribution sites.</li> <li>○ Provide training for reporting suspicious activity.</li> </ul> </li> <li>• Does the installation have a process to retrieve access media from employees of expired contracts?             <ul style="list-style-type: none"> <li>○ Is there a process to immediately retrieve access media for terminated contractors?</li> </ul> </li> <li>• Are site-specific measures developed to screen contractor or sub-contractors transportation conveyances for CBRNE hazards before entry into or adjacent to areas with DOD personnel and mission-essential assets? [Coordinate with Emergency Management/CBRNE specialist.]</li> </ul>	DOD Std 18
<b>AT MEASURES FOR CRITICAL ASSET SECURITY</b>		
SO-PLN-23	<p><b>Critical Asset Security.</b> Installation commanders shall develop and implement risk mitigation measures to reduce the vulnerabilities of DOD critical assets to terrorist attack and integrate these measures into overall AT program efforts.</p> <ul style="list-style-type: none"> <li>• Have security measures been developed for assets identified on the Mission-essential and/or vulnerable areas (MEVA) or Critical Asset list?</li> </ul> <p><b><u>ASSESSMENT OF CRITICAL FACILITIES</u></b></p> <ul style="list-style-type: none"> <li>• What is the design basis threat (weapons and tactics) for which the asset is to be assessed?</li> <li>• Are security measures based on threat, criticality, and vulnerability?</li> <li>• Are risk mitigation measures for critical assets included in the AT Plan as part of the Physical Security Program? [Coordinate with IE for critical infrastructure protection.]</li> <li>• Are drawings of the facility controlled to prevent the disclosure of sensitive information?</li> </ul>	DOD Std 19  Strategic Goal 2D

## FOR OFFICIAL USE ONLY

	<p><b><u>PLANNING</u></b></p> <ul style="list-style-type: none"><li>• Does the facility's Physical Security or AT Plan complement the installation's AT Plan and contain the minimum requirements outlined in the plan?</li><li>• Has the facility's Physical Security Plan been reviewed by the installation ATO?</li><li>• Is there a representative who attends the installation's ATWG (if tenant on the installation)?</li><li>• Does the facility have physical security plans that explain, at a minimum, how the facility will:<ul style="list-style-type: none"><li>○ Transition through each FPCON?</li><li>○ Participate in the installation's RAM program?</li><li>○ Control personnel access?</li><li>○ Control vehicle access, if applicable?</li><li>○ Implement barrier plans (coordinated with ATO)?</li><li>○ Implement bomb threat plans?</li></ul></li><li>• Are personnel identified to protect these assets during increased threats?</li></ul> <p><b><u>PERIMETER / EXTERIOR</u></b></p> <ul style="list-style-type: none"><li>• Are there any public access vantage points that allow potential aggressors to observe and target people or other assets in or around the building?</li><li>• Are there any signs that identify the criticality or sensitivity of the facility?</li><li>• If there are commercial transportation nodes closed to the facility, are there any procedures in place to prohibit stopping adjacent to the facility?</li><li>• Is the exterior of the facility clear from obstructions within 10 meters (33 feet) and does not provide concealment of explosive devices 150 mm (six inches) or greater in height?</li><li>• Are electrical and mechanical equipment provided enclosures to prevent placement and concealment of explosive devices?</li><li>• If parking garages are located underneath the facility, is access controlled for pedestrians and vehicles?</li><li>• Is sufficient lighting provided for vehicular and pedestrian entrances and perimeter? [Check backup power availability.]</li><li>• Does perimeter lighting provide continuous lighting on both sides of the perimeter barriers?</li><li>• Is lighting sufficient enough to support CCTV (if installed) operations and other surveillance?</li></ul>	
--	---	--

## FOR OFFICIAL USE ONLY

### ACCESS CONTROL FOR CRITICAL FACILITIES

- Has an access control system / access procedures been developed that can both delay attackers in reaching protected areas and inhibit egress from the facility?
- Are there Security Forces or other personnel performing access control to the facility?
- Have written standard operating procedures been developed for the guard post, to include emergency entry procedures?
- Do the Security Force members have a list of all personnel authorized access to the facility? If computer generated, is this process safeguarded against tampering?
- Is the access control list current?
- Is there a requirement to have the access control listing authenticated by someone in the Security Force chain of command?
- Are visitors pre-announced and verified once they arrive?
- Is package and personnel screening conducted at the access control point?
- Have the personnel performing access control received training on the security screening equipment?
- Do security personnel monitor access to mechanical, electrical, and telecommunication rooms?
- Has an access control roster been developed for the mechanical, electrical, and telecommunication rooms?
- Are facility CCTV systems installed at entrances, exits, vehicular entrances into parking garages, and loading docks?
- Is the system capable of being monitored at the Security Force control center as well as on-site? [Refer to Electronic Security System benchmarks.]
- Are there roving patrols interior/exterior assigned to the facility?
- Is there a duress alarm for the guard and/or other locations within the facility?
- Who responds to the duress alarm or any other incidents at the facility? What is the response time?
- Are personnel within the facility notified when the guard initiates his/her duress alarm?
- Will activation of the duress alarm lock down the facility?

**FOR OFFICIAL USE ONLY**

	<p><b><u>FACILITY BOMB THREAT PLAN</u></b></p> <ul style="list-style-type: none"> <li>• Have written bomb threat procedures been developed?</li> <li>• Are the procedures based on the installation’s requirements?</li> <li>• Do procedures identify primary and alternate rally points?             <ul style="list-style-type: none"> <li>○ Identify leadership and accountability procedures?</li> </ul> </li> <li>• Does the facility have a unique alert tone (separate from the fire alarm) to evacuate the facility?</li> <li>• Are new employees or building occupants trained on the bomb threat response procedures?</li> <li>• If a billeting area, are occupants provided information on the bomb threat plan?</li> <li>• Have search team members been identified and trained on search procedures?</li> <li>• Do all personnel have the installation’s version of the current bomb data collection sheet?</li> <li>• Has the installation ATO and/or EOD reviewed the bomb threat plan?</li> <li>• Are plans coordinated with adjacent facilities to avoid confusion during evacuation?</li> <li>• Is there an established frequency to exercise the bomb threat plan?</li> <li>• Are acceptable mail and parcel handling procedures being followed, to include screening, delivery, and response for expected explosive devices?</li> <li>• Are mail handlers properly trained in identifying mail and parcel bombs and exercises are being conducted to ensure personnel remain trained and alert?</li> </ul>	
SO-PLN-24	<p><b>Off-Installation Critical Assets.</b> Installation commanders shall coordinate with the appropriate local, state, federal, or host-nation authorities responsible for the security of non-DOD critical assets and overall capability of the DOD to execute the National Military Strategy. [Coordinate with Infrastructure Engineer.]</p> <ul style="list-style-type: none"> <li>• Has the Commander coordinated for the protection of non-DOD critical assets?</li> <li>• Do Security Forces coordinate with local law enforcement to provide security coverage of these assets?</li> </ul>	DOD Std 19  Strategic Goal 2D

**FOR OFFICIAL USE ONLY**

	<b>AT MEASURES FOR OFF-INSTALLATION FACILITIES, HOUSING, AND ACTIVITIES</b>	
SO-PLN-25	<p><b>Off-Installation facilities/activities.</b> Installation commanders shall develop in their overall AT programs specific AT measures for off-installation facilities, housing, and activities.</p> <ul style="list-style-type: none"> <li>• Has the Commander developed AT measures for the following off-installation activities: <ul style="list-style-type: none"> <li>○ Facilities (physical security measures)?</li> <li>○ Housing (guidance for selection / physical security measures)?</li> <li>○ Transportation Services (planning and route analysis)?</li> <li>○ Daycare centers (physical security measures)?</li> <li>○ Activities used by or involving mass-gatherings of DOD personnel and their family members.</li> </ul> </li> <li>• Does the installation have procedures to complete residential security reviews prior to personnel entering into formal contract negotiations for the lease or purchase of off-installation housing in Significant or High Threat Level Areas? (OCONUS)</li> <li>• Based on the physical security surveys, does the installation have procedures to provide AT recommendations to residents and facility owners?</li> <li>• Have Mutual Aid Agreements or other similarly structured protocols been developed with appropriate local, state, federal, and host-nation authorities to coordinate security measures and assistance requirements?</li> <li>• Are route maps of residences maintained at a 24 hour operating center? If not, is there a process to contact persons responsible for maintaining route maps in the event of an incident requiring the emergency notification of off-installation residents?</li> <li>• Do unit AT plans include current residence location information for all unit members residing off-installation?</li> <li>• Do incident response plans include measures for off-installation personnel (personnel warning system)?</li> </ul>	<p>DOD Std 15</p> <p>DOD O-2000.12-H, Chapter 22</p> <p>Strategic Goal 2F</p>
<b>TERRORIST INCIDENT RESPONSE / TERRORIST CONSEQUENCE MANAGEMENT</b>		
<b>[ coordinated with Emergency Management ]</b>		
SO-PLN-27	<p><b>Terrorism Consequence Management.</b> The Installation Commander shall develop a crisis management plan to respond to a terrorist incident.</p> <ul style="list-style-type: none"> <li>• Have the following items been included in crisis management planning? <ul style="list-style-type: none"> <li>○ Are special threat plans and physical security plans mutually supportive?</li> <li>○ Does the special threat plan include the threats identified in the threat statements of HHQ?</li> <li>○ Does the plan provide for a response for each phase of antiterrorism activity (e.g., initial response, negotiation, assault)?</li> <li>○ Does the plan take into consideration the movement from various locations, including commercial airports, of civilian and military advisory personnel with military transportation assets?</li> <li>○ Does the plan allow for the purchase and/or use of civilian vehicles, supplies, food, etc., if needed (including use to satisfy a hostage demand)?</li> <li>○ Does the plan make provisions for paying civilian employees overtime if they are involved in a special threat situation?</li> </ul> </li> </ul>	<p>DOD Std 20</p> <p>DOD O-2000-12-H, Chapters 11 and 12, AP5</p> <p>Strategic Goal 2D</p>

## FOR OFFICIAL USE ONLY

<b>3. ANTITERRORISM TRAINING AND EXERCISES</b>		
SO-TE-01	<p><b>AT Training and Exercises.</b> Installation commanders shall ensure that AT training and exercises are integrated with overall physical security and are afforded the same emphasis as combat task training and executed with the intent to identify shortfalls impacting the protection of personnel and assets against terrorist attack and subsequent consequence management efforts.</p> <ul style="list-style-type: none"> <li>• Is training provided to the Security Forces to conduct all phases of the installation's Physical Security Program?</li> <li>• Are training records maintained?</li> <li>• Are exercises conducted with the local responders?</li> </ul>	<p>DOD Std 23</p> <p>Strategic Goal 3F</p>
SO-TE-02	<p><b>Pre-deployment Training.</b> Installation commanders shall ensure that pre-deployment training is supported by measurable standards, including credible deterrence and response standards and deterrence-specific tactics, techniques, and procedures (TTP).</p> <ul style="list-style-type: none"> <li>• Does AT training include measurable standards?</li> <li>• Does training for deploying forces include deterrence, response standards, and deterrence-specific TTPs?</li> <li>• Is training for deploying forces documented?</li> <li>• Is training designed to meet gaining Commander's requirements?</li> <li>• Is AT training incorporated into unit-level training plans and pre-deployment exercises?</li> <li>• Are deploying members trained on local security procedures at the deployed location?</li> <li>• Are terrorist scenarios included in the pre-deployment training?</li> <li>• Are personnel involved in law enforcement / security trained in hostile intent decision-making?</li> <li>• Are deployed Commanders trained in hostile intent decision-making (i.e. ROE, use of force)?</li> </ul>	<p>DOD Std 23</p> <p>Strategic Goal 3B</p>
SO-TE-03	<p><b>Formal AT Training.</b> Installation commanders shall ensure all assigned personnel complete appropriate formal training and education. Individual records shall be updated to reflect completion of the AT training (Level I, II, III, and IV). Documentation of training should be in accordance with the DOD component's requirements.</p> <ul style="list-style-type: none"> <li>• Is there a process to ensure personnel received appropriate AT training?</li> <li>• Is there a documentation process for accomplished training?</li> <li>• Is there a process to ensure HRP's receive appropriate training?</li> </ul>	<p>DOD Std 24</p> <p>Strategic Goal 3E</p>
SO-TE-04	<p><b>Reporting AT Training Deficiencies.</b> Commanders and civilian equivalent directors, at all levels, who receive individuals not properly trained (AT, HRP, etc.) shall provide the required AT training as soon as practical. Concurrently, they shall provide the deficiency through the DOD components' chain of command to the losing DOD components, who shall institute appropriate corrective action to prevent reoccurrence of the discrepancy.</p> <ul style="list-style-type: none"> <li>• Is there a process to screen records of incoming personnel for AT training?</li> <li>• Is there a process to ensure personnel who have not received AT training are provided the training as soon as practical?</li> <li>• What is the process to report receipt of untrained personnel through the chain of command?</li> <li>• How are deficiencies being up channeled and to whom?</li> </ul>	<p>DOD Std 24</p> <p>Strategic Goal 3B</p>

**FOR OFFICIAL USE ONLY**

<p>SO-TE-05</p>	<p><b>Level I AT Awareness Training.</b> Installation commanders shall ensure that Level I AT Awareness training adheres to the minimum requirements listed in Table E3.T1 of DODI 2000.16.</p> <ul style="list-style-type: none"> <li>• Is Level I AT Awareness training provided in accordance with the curriculum described in DODI 2000.16?</li> <li>• Is individual awareness of terrorism threat sufficient for threat environment/mission?</li> <li>• Recommend localized individual protective measures be included as part of the Level I training?</li> <li>• Is there a method of tracking training to ensure all personnel have received the required training?</li> <li>• Is there a process to ensure all personnel annually receive Level I AT Awareness Training?</li> </ul> <p><b><u>FAMILY MEMBERS</u></b></p> <ul style="list-style-type: none"> <li>• Are family members provided Level I AT Awareness training for official travel?</li> <li>• Are family members encouraged to complete Level I AT Awareness training when traveling on other than official travel outside US or areas where the threat level is Moderate or higher?</li> </ul> <p><b><u>CONTRACTORS</u></b></p> <ul style="list-style-type: none"> <li>• Is the requirement to attend Level I included in contracts?</li> <li>• Are contractors afforded the opportunity to attend Level I training?</li> </ul> <p><b><u>Host-Nation/Third Country National</u></b></p> <ul style="list-style-type: none"> <li>• Does Level I AT Awareness Training include local nationals and third country nationals?</li> </ul>	<p>DOD Std 25</p> <p>JP 3-07.2</p> <p>Strategic Goal 3B</p>
<p>SO-TE-06</p>	<p><b>Level I Instructors.</b> Installation commanders shall designate in writing all individuals qualified to administer Level I AT Awareness Training.</p> <ul style="list-style-type: none"> <li>• Does the ATO maintain the list of those personnel qualified to administer Level I AT Awareness Training?</li> <li>• Are instructors certified using one of the following methods?             <ul style="list-style-type: none"> <li>○ Completion of a formal Military Service-approved Level II ATO Training Course of Instruction, whether resident or through a mobile training team.</li> <li>○ Completion of a DOD-sponsored and certified computer or web-based distance learning instruction course for Level II ATO Training. Applicable to DOD Agencies and field activities.</li> <li>○ Commanders and civilian equivalents may qualify Subject Matter Experts who have received formal training in AT TTP and individual protection and are knowledgeable in the current AT publications and methods for obtaining AOR-specific updates.</li> </ul> </li> <li>• Does the appointment letter for Commander-certified personnel clearly describe the qualifications of the individual and justify this method of certification? Additionally, does the letter explain why the other options are not feasible?</li> </ul>	<p>DOD Std 25</p>

**FOR OFFICIAL USE ONLY**

<p>SO-TE-07</p>	<p><b>ATO Level II Training.</b> Installation Antiterrorism Officers shall complete an approved Level II ATO Training Course.</p> <ul style="list-style-type: none"> <li>• Has the ATO completed an approved Level II ATO Training Course?</li> <li>• Reference E3.26.2.2in DOD 2000.16</li> </ul>	<p>DOD Std 26</p>
<p>SO-TE-08</p>	<p><b>AOR-Specific Training.</b> Installation commanders shall ensure that DOD personnel (including family members 14-years and older) departing to a Geographic Commander’s AOR complete the gaining COCOM’s AOR-specific AT education requirements within three months of a permanent change of station.</p> <ul style="list-style-type: none"> <li>• Is there a written process to ensure all personnel meet the gaining COCOM’s requirements?</li> <li>• Is there a mechanism used to ensure Permanent Change of Station personnel receive the AOR-specific brief within three months of departure?</li> <li>• Are AOR-specific requirements fulfilled for deployments?</li> <li>• Does the installation ensure intra-theater transiting units receive detailed threat information covering travel routes and sites that will be visited by the unit?</li> </ul>	<p>DOD Std 29</p> <p>Strategic Goal 3B</p>

## FOR OFFICIAL USE ONLY

<b>4. AT RESOURCE APPLICATION</b>		
SO-RA-01	<p><b>AT Resource Application Process.</b> The Installation commander shall identify AT resource requirements using the DOD-approved methodology for documenting and prioritizing AT resource requirements.</p> <ul style="list-style-type: none"> <li>• Does the installation’s AT resourcing process use the risk analysis (criticality, threat, and vulnerability) products for resource determination?</li> <li>• Is there a resource justification / prioritization process that incorporates the following:               <ul style="list-style-type: none"> <li>○ Threat?</li> <li>○ Asset Criticality?</li> <li>○ Asset Vulnerability?</li> <li>○ Current AT effectiveness?</li> <li>○ Impact on Plan / Programs?</li> <li>○ Mitigation Measures?</li> <li>○ Commander’s Risk?</li> </ul> </li> <li>• Is the prioritization focused on the most critical and important needs first?               <ul style="list-style-type: none"> <li>○ Resources necessary to meet minimal security requirements and to adhere to DOD Service directives, standards, instructions, or regulations.</li> <li>○ Resources required to mitigate a major or high-risk situation</li> </ul> </li> <li>• Is the ATWG involved in the prioritization of resource requirements?</li> <li>• Are the projected resource requirements:               <ul style="list-style-type: none"> <li>○ Affordable?</li> <li>○ Supportable?</li> <li>○ Risk reducing?</li> <li>○ Providing a high or moderate impact on the program to achieve the objectives identified in the AT Plan?</li> </ul> </li> <li>• Does the installation have an acquisition strategy to obtain funding sources?</li> <li>• Does resource cost include all life-cycle cost (manpower needs, logistics / maintenance, replacement cost)?               <ul style="list-style-type: none"> <li>○ Are AT resource requirements matched against other organization unfunded or funded requirements to determine if an internal reallocation of funding is appropriate and possible?</li> </ul> </li> <li>• Are unfunded requirements entered into the Core Vulnerability Assessment Management Program (CVAMP)?</li> </ul>	<p>DOD Std 30</p> <p>Strategic Goal 4C</p>
SO-RA-02	<p><b>CbT-RIF Submission.</b> The Installation Commander shall have procedures to adhere to the HHQ’s CbT-RIF submissions.</p> <ul style="list-style-type: none"> <li>• Does the installation’s process conform to the HHQ process and include installation-specific procedures? (HHQ guidance can be referenced in the installation AT Plan.)</li> <li>• Is there a plan to obligate funding within 90-days of receipt if CbT-RIF funds have been approved?</li> <li>• If CbT-RIF funds have been received, were they used as intended and were the vulnerabilities mitigated? [Coordinate with all team members and evaluate CVAMP.]</li> <li>• Are CbT-RIF submissions entered into CVAMP?</li> </ul>	<p>DOD Std 30</p> <p>CJCSI 5260.01D</p> <p>Strategic Goal 4B</p>

**FOR OFFICIAL USE ONLY**

SO-RA-03	<p><b>AT Technologies.</b> Installation commanders shall incorporate AT technologies into their AT program to enhance AT readiness, emergency preparedness, and improve CBRNE-related protective measures, specifically in the following categories:</p> <ul style="list-style-type: none"> <li>• Detecting and defeating improvised explosive devices.</li> <li>• Investigative / Forensics Support.</li> <li>• Physical Security.</li> <li>• Protecting Critical Infrastructure.</li> <li>• Personnel protection.</li> <li>• Training technology development.</li> <li>• Does the installation use technology to mitigate vulnerabilities where applicable? <ul style="list-style-type: none"> <li>○ Does the installation use the Antiterrorism Enterprise Portal (ATEP) to research available and tested technology?</li> </ul> </li> </ul>	DOD Std 13  Strategic Goal 4E
<b>5. COMPREHENSIVE AT PROGRAM REVIEW</b>		
SO-PR-01	<p><b>Comprehensive Program Review.</b> The Installation Commander shall conduct comprehensive AT Program Reviews to evaluate the effectiveness and adequacy of AT Program implementation. The evaluation shall include an assessment of the degree to which DOD component AT Programs comply with the standards prescribed in DODI 2000.16.</p> <ul style="list-style-type: none"> <li>• Has the installation defined a process to conduct Program Reviews?</li> <li>• Who has been designated to conduct the Program Reviews?</li> <li>• Has a tool (checklist, etc.) been developed for assessors, as required by component?</li> <li>• Does the assessment tool contain command-specific assessment items?</li> <li>• Does the Program Review process validate the thoroughness of the AT risk management methodology used to assess asset criticality, terrorist threat, and vulnerabilities? Is there a process to ensure program reviews are conducted on an annual basis?</li> <li>• Is there a process to conduct program reviews whenever there is a significant change in threat, vulnerabilities, or asset criticality necessitate?</li> <li>• Are tenants included in the Program Review?</li> </ul> <p><b><u>PRE-DEPLOYMENT PROGRAM REVIEW</u></b></p> <ul style="list-style-type: none"> <li>• Are Program Reviews conducted to ensure deploying units have viable AT programs and executable AT plans?</li> </ul>	DOD Std 31  DOD O-2000.12-H Chapter 15; API  Strategic Goal 5C
<b>ADDITIONAL PHYSICAL SECURITY BENCHMARKS PORT SECURITY</b>		

**FOR OFFICIAL USE ONLY**

SO-PS-01	<p><b>Port Security Plan.</b> The AT Plan should include a Port Security Plan for those installations with a body of water forming part or the entire perimeter. (See AT Planning Benchmarks.)</p> <ul style="list-style-type: none"><li>• The Port Security Plan should address:<ul style="list-style-type: none"><li>○ Policies</li><li>○ Plans</li><li>○ Procedures</li><li>○ Systems and equipment that will:<ul style="list-style-type: none"><li>▪ Detect</li><li>▪ Assess and classify threats</li><li>▪ Communicate warnings and threat assessment information</li><li>▪ Delay adversaries and provide for timely, effective response to a waterborne threat</li></ul></li><li>○ Barriers, lighting, CCTV and intrusion detection systems</li><li>○ Consideration to potential terrorist targets</li><li>○ Restricted areas</li><li>○ Use of patrol boats</li><li>○ Protection for sea approach choke points</li></ul></li><li>• Considers off-port observation points capable of observing port activities and the transit area.</li></ul>	DOD Std 7  DOD 5200.8-R  DOD O-2000.12-H, AP 17
----------	---	---

## FOR OFFICIAL USE ONLY

SO-PS-02	<p><b>Physical Security System.</b> Waterside physical security system should include barriers to establish a boundary, isolate activities, discourage visitors, and impede passage by boat or swimmer. [Coordinate with team Structural Engineer.]</p> <ul style="list-style-type: none"> <li>• Is there a Barrier Plan to complement waterside security?</li> <li>• Are barriers placed far enough from the assets to provide adequate protection based upon the design basis threat?</li> <li>• Do selected barriers provide surface and subsurface protection?</li> <li>• Are patrol boats incorporated into the Barrier Plan?</li> <li>• Are boats prohibited / prevented from coming within 500 meters of a DOD asset?</li> </ul> <p><b>SURVEILLANCE</b> - The waterside external surveillance must monitor traffic on the surface of the water adjacent to the facility, extending from the barrier to a range exceeding that of identified terrorist threat.</p> <ul style="list-style-type: none"> <li>• Does the facility have an external surveillance program?</li> <li>• Does the surveillance program extend beyond the capability of the waterborne threat?</li> <li>• Are areas under surveillance included in the security zone?</li> <li>• Does the surveillance program include central radar monitoring waterside area (warship radar, shipping/harbor control radar, expedient use of mast mounted radar on-shore)? Are lookouts posted topside on ships with night vision devices?</li> <li>• Are acoustic underwater sensors employed for surveillance purposes?</li> <li>• In high threat areas, is aerial surveillance employed?</li> </ul> <p><b>SECURITY ZONE</b> - A Security Zone shall be established within the surveillance area extending from the high-water mark to a distance at least 1,000 meters from the shore if possible.</p> <ul style="list-style-type: none"> <li>• Has an appropriate Security Zone been established?</li> <li>• Is the Security Zone based upon the Threat Assessment?</li> <li>• Has a reaction zone been established within the Security Zone?</li> <li>• Is the Security Zone developed to include multiple ships when present?</li> <li>• Have navigational aids mounted on structures in shallow water been included in the Security Zone (may also include airfield navigational aids in bays and rivers)?</li> <li>• Has the Security Zone been coordinated with the local / host government authorities?</li> <li>• Are local / host nation authorities involved in the enforcement of the Security Zone?</li> <li>• Is the Security Zone marked on navigational charts as well as aeronautical when there is a "Restricted Air Space"?</li> <li>• Has a "Restricted Air Space" been coordinated / established through the Transportation Security Administration (TSA) or host-government authorities?</li> <li>• Is the Security Zone prominently marked on the waterside?</li> </ul>	<p>DOD Std 13</p> <p>DOD O-2000.12-H, AP17.3</p> <p>DOD O-2000-12-H, C22.14.4</p> <p>DOD 5200 8-R</p>
----------	--	---

**FOR OFFICIAL USE ONLY**

	<p><b>Perimeter Security.</b> The port security perimeter must extend into the water if the threat assessment identifies a threat capable of launching a standoff weapon attack from boats or other crafts. [Coordinate with team Terrorist Operations Specialist]</p> <ul style="list-style-type: none"><li>• Has the Threat Assessment identified the threat of a standoff weapons attack from the water? [Coordinate with Terrorist Operations.]</li><li>• Does the security perimeter extend out beyond the distance of the weapon capability?</li><li>• Is the perimeter secured to prevent the threat from gaining access into the security perimeter to launch the standoff weapons attack?</li></ul> <p><b><u>CLASSIFICATION/ASSESSMENT</u></b></p> <ul style="list-style-type: none"><li>• Is there a process to classify the threat once an intruder has been detected?</li></ul> <p><b><u>RESPONSE</u></b></p> <ul style="list-style-type: none"><li>• Have Security Forces (i.e., organic security forces, U.S. Coast Guard, state or local police, host-government forces if overseas) been identified to respond to intrusions in the Security Zone?<ul style="list-style-type: none"><li>○ Is other law enforcement-type training provided (i.e., U.S. Coast Guard, Marine Patrols)?</li><li>○ Have lesson plans been developed to train personnel responsible for waterside security?</li></ul></li></ul>	<p>DOD Std 13</p> <p>DOD O-2000-12-H, C22.14.4, AP 17</p>
--	---	---

**FOR OFFICIAL USE ONLY**

SO-PS-03	<p><b>Coordination for Waterside Security.</b> Coordination shall be conducted with federal, state, and local agencies; law enforcement and security agencies; and port stakeholders.</p> <ul style="list-style-type: none"> <li>• Have support agreements been developed with the local law enforcement and other port authorities for support during terrorist incidents?</li> <li>• Have the provisions of the agreements been validated through a practical exercise?</li> <li>• Is joint training conducted between all responding forces?</li> </ul>	<p>DOD Std 8</p> <p>DOD 5200 8-R</p>
SO-PS-04	<p><b>Ships outside of Homeport.</b> Prior to a ship pulling into any port outside of its homeport, the ship shall have an in-port force protection plan approved by the appropriate Commander.</p> <ul style="list-style-type: none"> <li>• Is there a process to ensure all departing ships have an approved in-port force protection plan?</li> <li>• Is there a demarcation zone that identifies the area where watch standers may engage targets?</li> <li>• Is there a communications plan for watch standers?</li> <li>• Are rules of engagement established?</li> </ul>	<p>DOD Std 7</p> <p>DOD O-2000.12-H, Chapter 22, AP3.2 .1.2</p>
SO-PS-05	<p><b>Deployed Ships.</b> Is there a security watch for deployed ships that provides safeguards from sabotage, terrorism, civil disturbance, danger, or compromise?</p> <ul style="list-style-type: none"> <li>• Has the Commander established a security watch?</li> <li>• Is an Officer of the Deck (OOD) or equivalent appointed, and does he have the responsibility for posting all security watches/sentries?</li> <li>• Are all watch standers bearing arms properly qualified?</li> <li>• Are watch standers trained in hostile decision-making?</li> <li>• Is there an alert process to notify shipboard personnel of attempts to board ship at locations other than brows, sea ladders, or normal access areas?</li> <li>• Are watch standers provided written access control procedures to board the ship? Personnel should be denied access until cleared by the ODO.</li> </ul>	<p>DOD Std 13</p> <p>DOD O-2000.12-H, Chapter 22, AP3.2 .1.3</p>

## FOR OFFICIAL USE ONLY

SO-PS-06	<p><b>Deliveries.</b> Material brought aboard ship shall be randomly inspected by watchstanders, designated members of the Master-at-Arms force, or other petty officers trained in proper inspection procedures. (Use Access Control Benchmarks to support this Benchmark.)</p> <ul style="list-style-type: none"> <li>• Is there a process to randomly inspect materiel prior to being brought on board?</li> <li>• Are personnel performing these inspections trained in search techniques?</li> <li>• Is there a process to incorporate technology and/or explosive detection dogs into the random inspection process?</li> </ul>	<p>DOD Std 13</p> <p>DOD O-2000.12-H, Chapter 22, AP3.2 .1.5</p>
SO-PS-07	<p><b>Deploying Ships.</b> Deploying ships shall accomplish pre-deployment procedures. (Also use pre-deployment VA and Training Benchmarks.)</p> <ul style="list-style-type: none"> <li>• Do pre-port procedures include the following: <ul style="list-style-type: none"> <li>○ Obtaining a current Threat Assessment from the local NCIS representative?</li> <li>○ Senior commander issuing security requirements for all ships?</li> <li>○ Briefing crew on threat, security precautions, recall procedures, and ship's Self Defense Force (SDF) duties?</li> <li>○ Briefing security forces, briefing threat specifics, and reviewing the rules of engagement or use of force policies, security assignments, and responsibilities?</li> <li>○ Briefing beach guards and shore patrols on threats and reviewing special procedures applicable to the specific port visit, including pier and/or fleet landing security and access control procedures?</li> <li>○ When operating under FPCON BRAVO in non-Navy ports, or when a threat to a specific ship is received, using a MWD and divers to conduct a search of the pier prior to the ship's arrival, when available?</li> </ul> </li> </ul>	<p>DOD Std 13</p> <p>DOD O-2000.12-H, Chapter 22, AP3.2 .1.6</p>
SO-PS-08	<p><b>Contracting.</b> Ensure that minimum hiring standards and procedures are maintained for port personnel, including security, longshoremen, management, etc. The procedures should include local background checks before hire, routine updates, follow up on discrepancies, etc. Hiring standards and procedures should be considered for all contract negotiations, particularly in OCONUS. (See Contracting and Logistics Benchmarks.)</p> <ul style="list-style-type: none"> <li>• Is there a process to ensure trustworthiness of non-DOD personnel supporting ship operations?</li> <li>• Does the process include follow-up investigations?</li> <li>• Is this process incorporated into the contract?</li> </ul>	<p>DOD Std 13</p> <p>DOD O-2000.12-H, Chapter 22, AP3.2</p>
<b>ADDITIONAL PHYSICAL SECURITY BENCHMARKS – AIRFIELD SECURITY</b>		
SO-AS-01	<p><b>Airfield Security Plan.</b> The AT Plan shall include plans for protection of airfields located on the installation. (Reference AT Planning Benchmarks.)</p> <ul style="list-style-type: none"> <li>• Does the plan address: <ul style="list-style-type: none"> <li>○ Access control?</li> <li>○ Intrusion detection systems?</li> <li>○ Barrier Plan?</li> <li>○ Airfield-specific FPCON measures ?</li> <li>○ Security response?</li> <li>○ Expanded Security Operations?</li> </ul> </li> <li>• Does the airfield security plan incorporate support identified in the installation AT plan?</li> </ul>	<p>DOD Std 7</p> <p>DOD 5200 8 R</p> <p>DOD O-2000.12-H, Chapter 22, C22.12</p>

**FOR OFFICIAL USE ONLY**

<p>SO-AS-02</p>	<p><b>Physical Security System.</b> Installation Commander shall provide protection of DOD assets located on installation airfields.</p> <ul style="list-style-type: none"> <li>• Does airfield security consist of the following components:             <ul style="list-style-type: none"> <li>○ Multiple internal security perimeters?</li> <li>○ Hardening of selected buildings against terrorist attacks?</li> <li>○ Hardening of petroleum storage?</li> <li>○ Aircrew facilities?</li> <li>○ Maintenance facilities?</li> <li>○ Other collocated facilities?</li> </ul> </li> <li>• Is airfield security planning IAW applicable HHQ requirements?</li> <li>• Are runway and taxiways included in the protection scheme, to include the utilities that may be buried beneath them? [Coordinate with Infrastructure Engineer.]</li> <li>• Are aircraft in maintenance provided appropriate protection, security forces, or maintenance personnel?</li> </ul> <p><b><u>PARKING AREA/ACCESS CONTROL</u></b></p> <ul style="list-style-type: none"> <li>• Are aircraft parked within a restricted/controlled area?</li> <li>• Is there a separate airfield perimeter fence (requirement depends on type of resource and installation perimeter)?</li> <li>• Is positive access control provided for sensitive airfields (e.g., Priority Level resources, alert aircraft, and DV aircraft)?</li> <li>• Is there an identification system that allows access to the flight line for vehicles and personnel?</li> <li>• Are barriers in place to control vehicle access?</li> <li>• Are high-speed approaches mitigated?</li> <li>• Are access control points randomly manned?</li> <li>• Do Security Forces conduct random credential checks in the flight line area?</li> <li>• Are parking areas prominently marked with warning signs?</li> <li>• Is there a process to limit vehicle access points for increased threats?</li> </ul> <p><b><u>INTRUSION DETECTION SYSTEM (IDS)</u></b> Use ESS Benchmarks</p> <ul style="list-style-type: none"> <li>• Are multiple layers of IDS used on the airfield (line detectors, motion detectors mounted on fences, and seismic or acoustic sensors sown in patterns)?</li> <li>• Are airfield electronics protected (i.e., devices to support aircraft takeoffs and landings in all weather and visibility conditions)?</li> <li>• Is beyond-the-perimeter surveillance incorporated into the airfield security planning?</li> <li>• Are special aircraft equipped with IDS?</li> </ul>	<p>DOD Std 13</p> <p>DOD 5200 8-R, Chapter 4</p> <p>DOD O-2000.12-H, Chapter 22, C22.12</p>
-----------------	--	---

**FOR OFFICIAL USE ONLY**

<p>SO-AS-03</p>	<p><b>Man-Portable Air Defense System (MANPAD).</b> Procedures to mitigate MANPAD threats should be developed.</p> <ul style="list-style-type: none"> <li>• Has a MANPAD Risk Assessment been conducted to identify areas vulnerable to a MANPAD threat (possible launch sites)?</li> <li>• Have contingency plans been developed to respond to MANPAD threats?</li> <li>• Does the AT Plan address the following considerations:             <ul style="list-style-type: none"> <li>○ Establishes airfield-specific procedures (contained in the FPCON measures) for the use of aircrew tactical countermeasures and/or tactics? Includes coordination with the local / host nation authorities.</li> <li>○ Incorporates current airfield threat and security assessments, especially for deployments?</li> <li>○ Varying arrival and departure times of aircraft?</li> <li>○ Randomly changing approach and departure routes as a deterrent (IAW current TSA guidelines)?</li> <li>○ Limiting or discontinuing use of landing lights within identified threat zones?</li> <li>○ For high threat areas, coordinating and developing plans for engine running offloads to minimize ground time?</li> </ul> </li> <li>• Has the installation employed tools such as the AMC Intelligence Combined Risk Assessment database and the Flight Path Threat Analysis Simulation (FPTAS) into MANPAD planning?</li> <li>• Has an observation post on and off base been designated?             <ul style="list-style-type: none"> <li>○ Off-base observation post should be coordinated with local authorities.</li> </ul> </li> </ul> <p><b><u>COUNTERMEASURES</u></b></p> <ul style="list-style-type: none"> <li>• Has MANPAD defense been included in the AT Plan, and does this defense include the following:             <ul style="list-style-type: none"> <li>○ Increased physical presence at prime launches sites? Visual observations of security teams is a strong deterrent.</li> <li>○ Focused and random patrols of vulnerable areas? Random patrols should be part of the installation random AT measures program.</li> <li>○ Implementation of technical surveillance of vulnerable areas, to include both launch sites and potential targets?</li> <li>○ Ensuring personnel are educated on MANPAD threat (to include component recognition), areas of vulnerability, and reaction plans?                 <ul style="list-style-type: none"> <li>▪ MANPAD awareness training for Security Force personnel and local / host nation law enforcement.</li> <li>▪ MANPAD awareness program for neighborhood watch groups and local businesses / installation facilities in close proximity to airfields or along flight paths.</li> </ul> </li> <li>○ Ensuring tight airfield access control procedures are in place for airfield operations? Consider dispersal of parked aircraft to reduce damage from a MANPAD or RPG.</li> </ul> </li> <li>• Developing and exercising contingency plans for responding to an incident of a MANPAD threat.</li> </ul>	<p>DOD Std 13</p> <p>DOD 5200 8-R</p> <p>DOD O-2000.12-H, Chapter 22, C22.13</p>
-----------------	--	--

## FOR OFFICIAL USE ONLY

SO-AS-04	<p><b>Deployed Aircraft.</b> Commanders shall provide protection for deployed aircraft and crews. [Refer to pre-deployment VA and Training Benchmarks.]</p> <ul style="list-style-type: none"><li>• Are the following procedures implemented for deployed aircraft:<ul style="list-style-type: none"><li>○ Assign an ATO?</li><li>○ Assess threat for all locations the aircraft(s) and crews will visit?</li><li>○ Determine availability of Security Forces at all stops?</li><li>○ Determine detection capability at the deployed location?</li><li>○ Determine access control procedures at deployed location?</li><li>○ Determine response capability for enroute stops and those in place at the final destination?</li><li>○ Protect deployment itinerary?</li><li>○ Develop procedures to implement when provided security is inadequate (e.g., don't leave aircraft unattended, procedures to lock up aircraft if it has been left unattended)?</li><li>○ Tailored security measures to meet unique requirements when necessary (e.g. lock hatches and entry points, secure with tamper indicators, dress security personnel in aircrew uniforms, concealed weapons vice open carry)?</li><li>○ Coordinate Security Force requirements if aircraft deploys Security Forces (e.g., weapons storage, communications, vehicles, security equipment)?</li><li>○ Plan for deployed sensors?</li><li>○ Plan security for housing deployed personnel, to include transportation to and from airfield?</li></ul></li></ul>	DOD Std 13  DOD O-2000.12-H Chapter 22
----------	---	---

**FOR OFFICIAL USE ONLY**

**Annex C**  
**Structural Engineering Benchmarks**

<b>1. AT RISK MANAGEMENT</b>		
SE-RM-01	<p><b>Risk Management:</b> The essential components of Terrorism Risk Management include: assessing the terrorist threat; determining the criticality of assets; identifying the vulnerabilities of facilities, programs, and systems to terrorist attack; and outlining capabilities to deter terrorist incidents, employing countermeasures, and mitigating and recovering from the effects of a terrorist incident attack. [Coordinate with Security and Terrorist Operations.]</p> <ul style="list-style-type: none"><li>• Has the installation integrated a design basis threat (DBT) into their planning process?</li><li>• Are engineers part of the local vulnerability assessment (VA) team?</li><li>• Is the DBT used when conducting VAs?</li><li>• Are engineering considerations, to include general building construction, used when evaluating the effectiveness of countermeasures?</li><li>• Has the assessment been translated into action items for either resourcing or procedural corrections?</li><li>• Is the engineering department familiar with the prioritization of structures, and do their plans match the critical assets and infrastructure?</li><li>• Have Service and/or COCOM waivers been requested where risk has been accepted (if required)?</li></ul>	JP 3-07.2 DOD Std 3 DOD O-2000.12-H Strategic Goal 1H

**FOR OFFICIAL USE ONLY**

<b>2. AT PLANNING</b>		
SE-PLN-01	<p><b>Engineering Support to the AT Program:</b> Engineering support shall be included in the AT Program and discussed in the AT Plan.</p> <ul style="list-style-type: none"> <li>• Does engineering support to the AT Program integrate HHQ guidance (DOD, COCOM, Service)?</li> <li>• Has an appropriate entity been tasked in the AT Plan to provide engineering support to the AT Program?</li> <li>• Are engineering tasks spelled out and adequate to support the AT Program (e.g. design review process, construction criteria, Barrier Plan, maintenance of security technology [active barriers], and recovery actions)?</li> <li>• Is a prioritized list of AT factors, including facility-specific DBT, layout of the facility, Barrier Plan, standoff and construction, and site evaluation/selection criteria, identified in the AT Plan?               <ul style="list-style-type: none"> <li>○ Is the engineering department able to execute these tasks?</li> </ul> </li> <li>• Are engineers aware of critical assets and MEVAs, and are these assets incorporated in planning decisions? (Integrated Priority List (IPL): focusing resources on the most critical assets.)</li> <li>• Have COCOM and/or Service waivers been requested where necessary and permitted?</li> <li>• Does the AT Plan establish coordination responsibilities between the AT staff, physical security, and engineers?</li> <li>• Have security and engineering personnel been trained in Security Engineering criteria IAW COCOM or Service requirements?</li> <li>• Have security and engineering personnel attended a “Security Engineering Course” IAW COCOM requirements?</li> <li>• Do security and engineering personnel have a training plan to ensure they maintain proficiency?</li> <li>• Are security and engineering personnel aware of the latest technological developments in order to select appropriate and cost-effective counter measures?</li> <li>• Are security and engineering personnel familiar with blast analysis software programs and/or tools to aid in the development of barrier plans, construction requirements, and mitigation strategies or countermeasure selection?</li> <li>• Are engineers part of the ATWG?</li> </ul>	<p>DOD Std 7</p> <p>DOD O-2000.12-H</p> <p>Strategic Goal 2D</p> <p>UFC 4-020-01</p>

**FOR OFFICIAL USE ONLY**

<p>SE-PLN-02</p>	<p><b>Barrier Plan:</b> The Installation Commander shall integrate barriers into all physical security systems. Implementation of the Barrier Plan should be considered at FPCON BRAVO and is mandatory at FPCON CHARLIE and DELTA. The Barrier Plan shall be reviewed annually.</p> <ul style="list-style-type: none"> <li>• Has a Barrier Plan been developed at the installation, facility, or ship level?</li> <li>• Is the Barrier Plan based on a stationary or moving vehicle as defined by the DBT?</li> <li>• Has the installation considered and/or incorporated permanent physical standoff for critical assets / MEVAs identified in the Criticality Assessment?</li> <li>• Does the Barrier Plan support procedural security requirements?</li> <li>• Is the Barrier Plan based upon the DBT or other threat factors (criminal, FIS, etc.)?</li> <li>• Does the barrier system mitigate the identified threats?</li> <li>• Is the Barrier Plan written to clarify “who, what, when, and where” to assist in carrying out mitigation strategies including barrier placement, ACPs, and alternate parking?</li> <li>• Are tenants included in the Barrier Plan? Who will place barriers for tenant facilities?</li> <li>• Has the Barrier Plan been coordinated with key AT stakeholders (e.g. ATO, physical security, logistics, engineers, first responders)?</li> <li>• Is there a sufficient barrier inventory on hand to implement the Barrier Plan? Does the installation have a ready source for additional barriers?</li> </ul>	<p>DOD Std 7 JP 3-07.2 DOD O-2000.12-H Strategic Goal 2D</p>
------------------	--	--

**FOR OFFICIAL USE ONLY**

	<b>PLANNING AND NEW CONSTRUCTION</b>	
SE-PLN-03	<p><b>Unified Facilities Criteria (UFC):</b> The cost of incorporating antiterrorism principles into new construction and renovation projects are least in the early design phases. Installation planners should be familiar with the current UFC 4-010-01 and 4-010-02 standards and COCOM requirements in order to incorporate them into all DOD inhabited buildings, billeting, primary gathering buildings (PGB), MEVAs, and DOD expeditionary / temporary structures. All projects, regardless of funding, must comply with the latest DOD Construction Standards. Refer to UFC 4-010-01 for all limitations and applicability.</p> <p>The AT program shall establish procedures to adhere to common criteria and minimum construction (new, renovations, or rehabilitation) standards designed to mitigate AT vulnerabilities and threat. This process should provide guidance during all stages of construction planning and execution.</p> <p>New construction and renovation projects for billeting, PGB, and inhabited facilities should include an antiterrorism review at all stages of planning, programming, design, and construction. Review selected DD Forms 1391 to ensure antiterrorism is adequately covered and supports installation plans.</p> <ul style="list-style-type: none"> <li>• Are there procedures established and identified in the AT Plan to incorporate AT construction standards? (Adopt or supplement UFC.)</li> <li>• Does the AT Plan address coordination between the installation and tenant units to ensure AT construction criteria, DBT mitigation, facility layout, Barrier Plan, standoff, and site evaluation / selection criteria are addressed?</li> <li>• Has the installation incorporated the mandatory 22 standards from UFC 4-010-01, Appendix B?</li> <li>• Has the installation considered incorporating the 17 recommendations from UFC 4-010-01, Appendix C?</li> <li>• Are planners, designers, engineers, and security personnel aware of the latest DOD AT Standards, UFC, and COCOM criteria?             <ul style="list-style-type: none"> <li>○ Are COCOM AOR and/or country-specific AT construction standards / guidance incorporated into the facility planning process?</li> </ul> </li> <li>• Is there a process in place to perform formal reviews of projects by the appropriate personnel?</li> <li>• Are there line items (primary facility and supporting facilities) on the programming documents (e.g. DD Form 1391) indicating the added cost of AT measures?</li> </ul>	<p>DOD Std 17</p> <p>DOD O-2000.12-H</p> <p>Strategic Goal 2I</p> <p>UFC 4-010-01 &amp; 4-010-02</p> <p>UFC 4-022-01</p> <p>UFC 4-023-03</p> <p>COCOM OPOD</p>

## FOR OFFICIAL USE ONLY

	<p>Landscaping around critical facilities, troop billeting, and primary gathering buildings should not provide concealed areas.</p> <ul style="list-style-type: none"> <li>• Is landscaping considered during facility planning? [Engineering and security review.]</li> <li>• Does foliage obscure hidden packages (i.e. higher than 6")?</li> <li>• Is there a maintenance or service plan to control vegetation and shrubs?</li> </ul> <p>For troop billeting, PGBs, and inhabited buildings, drive-up or drop-off areas should be configured so vehicular access can be restricted at higher FPCONs.</p> <ul style="list-style-type: none"> <li>• Do drive-up and drop-off areas have provisions for restricting access?             <ul style="list-style-type: none"> <li>○ Are barriers adequate to prevent unauthorized entry?</li> </ul> </li> <li>• Does the FPCON Barrier Plan eliminate drive-up and drop-off areas?</li> </ul> <p>Central mail handling facilities should be sufficiently separated from inhabited structures and constructed IAW UFC requirements.</p> <ul style="list-style-type: none"> <li>• Is the mail room located away from high occupancy buildings and critical infrastructure?</li> <li>• Does it meet DOD UFC criteria?</li> <li>• Have blast protection measures been integrated into the mailroom facility design?</li> </ul>	
	<b>STANDOFF</b>	
	<p>The most effective protection from a bomb blast is standoff. Standoff is the distance between an inhabited building (target) and the closest point of a weapon. If adequate standoff is available, additional hardening measures will likely not be required. For a JSIVA, the assessment of standoff is divided into three parts: perimeter standoff, facility standoff, and vehicle barrier plans. Perimeter standoff refers to the distance measured from an installation perimeter to the closest point on the building exterior. This distance identifies how close to a structure a vehicle bomb can be placed without actually entering the installation. Facility standoff is the distance from the edge of pavement, parking area, or thoroughfare to the nearest face of a given structure. Vehicle barrier plans indicate how an installation will limit vehicle access during periods of increased threat and shows alternate parking methods such as centralized and off-base parking. As an installation elevates its FPCON, the Barrier Plans should become more restrictive, preventing vehicle movement into vital areas of the installation.</p>	

**FOR OFFICIAL USE ONLY**

	<b>PERIMETER STANDOFF</b>	
--	---------------------------	--

**FOR OFFICIAL USE ONLY**

<p>SE-PLN-04</p>	<p><b>Perimeter Standoff:</b> Distances between the installation's (controlled or uncontrolled) perimeter and inhabited buildings should be appropriate to the use, type of construction, and population of the building and the DBT.</p> <ul style="list-style-type: none"> <li>• Is perimeter controlled or uncontrolled? A physical boundary will be considered sufficient means to channel vehicles to the access control points. At a minimum, access control at a controlled perimeter requires the demonstrated capability to search for and detect explosives. Where the controlled perimeter includes a shoreline and there is no defined perimeter beyond the shoreline, the boundary will be at the mean high water mark.</li> <li>• What features define the perimeter? Does the perimeter have a vehicle barrier? If so, what kind of vehicle barrier is present?</li> <li>• Are perimeter standoff distances IAW building occupancy, construction, and population?             <ul style="list-style-type: none"> <li>○ Does the available distance between the controlled perimeter and the facility provide the level of protection required from the DBT?</li> <li>○ If not, have mitigating measures (curtailment, building hardening, etc.) been implemented to reduce the impact?</li> </ul> </li> <li>• Do off-base housing facilities have the standoff if required by the COCOM OPOD?             <ul style="list-style-type: none"> <li>○ If not, are compensatory measures in place to reduce the effects of an attack?</li> <li>○ Have waivers been requested (if applicable)?</li> </ul> </li> </ul> <p>Adjacent land use should be evaluated to determine the need for obscuration screening or additional measures.</p> <ul style="list-style-type: none"> <li>• Are facility entrance doors positioned so they cannot be easily targeted from the installation perimeter or uncontrolled vantage points?</li> <li>• Can a direct line of sight be avoided by obscuration screening, planting trees, or other methods?</li> </ul>	<p>DOD Std 17</p> <p>DOD O-2000.12-H</p> <p>Strategic Goal 2I</p>
------------------	--	---

## FOR OFFICIAL USE ONLY

ACCESS CONTROL POINTS		
SE-PLN-05	<p><b>Access Control Points (ACP):</b> The overall layout, organization, infrastructure, and facilities of an ACP should be capable of providing positive vehicle control and support access control procedures (vetting, inspection, and rejection.) ACPs should secure the installation from unauthorized access and the introduction of weapons while maximizing vehicular traffic flow and providing protection to personnel performing security functions at the ACP.</p> <p>UFC 4-022-01 is a design guide that provides information on desired features of an effective ACP. US Army standard definitive design for ACPs outlines mandatory features required for ACPs at US Army installations.</p> <ul style="list-style-type: none"> <li>• The Approach Zone should incorporate roadway layout and traffic control devices such as signs, variable message systems, signals, and lane control markings to notify drivers of the upcoming access control point, the proper speed to travel, and proper lane to utilize. Factors to consider include: <ul style="list-style-type: none"> <li>○ Are speed reduction / detection devices used to slow incoming vehicles to, or below, the design speed of the Access Control Point (ACP)?</li> <li>○ Is the capability to sort traffic by vehicle type into the proper lane before reaching the inspection area or checkpoint integrated into the ACP?</li> <li>○ Is adequate stacking distance provided for vehicles waiting for entry?</li> <li>○ Can security personnel identify potential threat vehicles, including those attempting entry through the outbound lanes of traffic?</li> </ul> </li> <li>• The Access Control Zone is the main body of the ACP and includes guard facilities and traffic management equipment used by the security personnel. Factors to consider include: <ul style="list-style-type: none"> <li>○ Are devices in place to allow security personnel to maintain positive control of vehicles when performing vehicle and personnel identification?</li> <li>○ Does the ACP include a specific area for vehicle inspections? This area must incorporate positive vehicle control, facilitate the inspection process, provide security for inspecting personnel, obscurity from surveillance, accommodate one or more vehicles requiring inspection, and include rejection capability.</li> <li>○ Can the ACP support tandem processing to limit the number of vehicles stacked in the approach zone?</li> <li>○ In addition to supporting manual procedures, does the design accommodate the use of automated identification systems? This includes channeling vehicles into the proper lanes and infrastructure support.</li> </ul> </li> <li>• The Response Zone is the area extending from the end of the Access Control Zone to the final denial barrier (FDB). Factors to consider include: <ul style="list-style-type: none"> <li>○ Does the response zone provide the time and space needed to allow security force personnel, including over watch positions, to react to a threat? This may include the use of traffic control and slowing devices, tire shredders distance, etc., for both incoming and exit lanes.</li> <li>○ Are FDBs incorporated into the ACP?</li> </ul> </li> <li>• The Safety Zone extends from the passive and active barriers in all directions to protect installation personnel from an explosion at the vehicle barricade. Factors to consider include:</li> </ul>	<p>DOD Std 13</p> <p>DOD O-2000.12-H</p> <p>Strategic Goal 2I</p> <p>UFC 4-010-01 &amp; 4-010-02</p> <p>UFC 4-020-01</p> <p>UFC 4-022-01</p>

**FOR OFFICIAL USE ONLY**

	<ul style="list-style-type: none"> <li>○ Does each ACP offer minimum standoff distance from billeting, MEVAs, critical facilities, and primary gathering buildings IAW DOD requirements?</li> <li>● Personnel protection must be integrated into the ACP design. Factors to consider include:             <ul style="list-style-type: none"> <li>○ Does each ACP have hardened guardhouse with bullet resistant doors, window frames, and glazing IAW DOD and COCOM OPORD requirements?</li> <li>○ Are devices in place to protect personnel from oncoming vehicles (bollards, high curbs, walls, or other barriers)?</li> </ul> </li> <li>● Other considerations include:             <ul style="list-style-type: none"> <li>○ Are barriers appropriate considering climate and terrain?</li> <li>○ Are barriers listed on either the DOD or DOS-certified anti-ram vehicle barrier list?</li> <li>○ Is obscuration incorporated into ACP design to limit hostile surveillance?</li> <li>○ Are there an appropriate number of ACPs for the quantity and type of traffic (employee, visitor, and commercial)?</li> <li>○ Are the ACPs sited appropriately considering demand for access to the installation, traffic origin and destination, capability of surrounding road networks, and security?</li> <li>○ Is there backup power for lights, FDBs, etc, or the provision to provide it via a portable generator?</li> <li>○ Is there a maintenance/repair program for physical security features?</li> </ul> </li> <li>● Unmanned / unused ACPs / gates:             <ul style="list-style-type: none"> <li>○ Are ACPs / gates secured to at least the same level as the adjoining fence?</li> <li>○ Are devices in place to prevent surreptitious vehicle entry?</li> <li>○ Are barriers used at unmanned ACPs / gates listed on either the DOD or DOS-certified anti-ram vehicle barrier list?</li> <li>○ Are high speed vehicular approaches eliminated?</li> </ul> </li> </ul>	
	<p><b>FACILITY STANDOFF</b></p>	
<p>SE-PLN-06</p>	<p><b>Facility Standoff:</b> For inhabited buildings, troop billeting, PGBs, and MEVAs, parking areas and vehicle access should be appropriate to the use, type of construction, population of the building, and the DBT. Provide the minimum standoff distance required in the UFC for the structure category of the building. The minimum standoff required is based on whether the perimeter is controlled or uncontrolled.</p> <ul style="list-style-type: none"> <li>● Have compensatory measures been implemented to protect critical assets/MEVAs IAW the Criticality Assessment if they do not have a controlled perimeter (permanent physical standoff)?</li> <li>● Is standoff appropriate for DBT, construction, and level of protection?</li> <li>● Is parking controlled and how?</li> </ul> <p>Trash containers and other containers that could conceal an improvised explosive device (IED) should be located an appropriate distance away from the building based on the use, type of construction, and population of the building.</p> <ul style="list-style-type: none"> <li>● Are trash containers located away from buildings?             <ul style="list-style-type: none"> <li>○ What is the standoff distance?</li> <li>○ Are trash containers secured?</li> </ul> </li> </ul>	<p>DOD Std 17</p> <p>DOD O-2000.12-H</p> <p>Strategic Goal 2I</p>

**FOR OFFICIAL USE ONLY**

	<p>Critical facilities, troop billeting, and PGBs should not be located near large non-DOD populations.</p> <ul style="list-style-type: none"><li>• Has adequate standoff been established IAW the UFC?</li><li>• Is obscuration used to prevent surveillance?</li><li>• Have buildings in this category been included in FPCON measures to establish additional standoff and/or curtailment requirements? Have barriers been installed around buildings?</li></ul> <p>Inhabited facilities should not have parking below or on top of the building.</p> <ul style="list-style-type: none"><li>• Is parking is allowed on top of or under the building?</li><li>• If so, how is vehicle access to these parking areas controlled?</li><li>• Has the building been hardened for blast resistance?<ul style="list-style-type: none"><li>○ Is building designed to resist progressive collapse?</li><li>○ Do restricted parking areas have adequate physical access control?</li></ul></li></ul>	
--	---	--

## FOR OFFICIAL USE ONLY

<b>BUILDING CHARACTERISTICS</b>		
	Existing building construction shall be assessed to determine an installation's vulnerability to weapons and the appropriateness of various mitigation measures. The type of construction has an effect on the protection afforded occupants in a terrorist bombing, standoff considerations, real property upgrades, and FPCON measures. Building characteristics data collected will be used to perform estimated building blast damage analysis calculations and to identify possible building and site modifications to mitigate the DBT.	
SE-PLN-08	<p><b>Existing Buildings:</b> Determine the construction materials used for inhabited buildings, billeting, PGBs, and MEVAs, noting glazing and exterior wall, frame, floor, and roofing systems. For targeted buildings, consider gathering the following information:</p> <ul style="list-style-type: none"> <li>• What is the typical construction of building components? <ul style="list-style-type: none"> <li>○ Walls: structural concrete, reinforced or un-reinforced CMU, load bearing brick or CMU, metal stud walls with exterior façade of brick or stucco</li> <li>○ Framing: floor slab, columns, beams, and roof</li> <li>○ Steel/concrete/wood/: beam size, columns, floor and roof deck</li> <li>○ Beam and column spacing</li> <li>○ Number of building floors and floor to ceiling/roof distances</li> <li>○ Size and numbers of exterior windows</li> <li>○ Window glazing type: annealed, tempered, and/or laminated; number of panes of glass and thickness of glass</li> <li>○ Has fragment retention security film been installed on the windows?</li> <li>○ Do the windows have blast curtains? Are the blast curtains normally kept closed?</li> <li>○ Obtain floor and site plan of buildings; obtain best available overhead imagery of buildings</li> <li>○ How many DOD personnel are typically in the building? What is the peak DOD population in the building? What is the total number of people in the building?</li> </ul> </li> <li>• Do windows have hardening system(s) IAW COCOM requirements?</li> <li>• Are there special regional design considerations (earthquake, hurricane, etc.) that may provide structural benefit in the case of an explosion?</li> <li>• Is there possibility of progressive collapse of any critical building (three story buildings or taller)?</li> <li>• Are exterior walls capable of resisting the DBT? If not, have exterior walls been retrofitted to resist the DBT? What was the retrofit method?</li> </ul>	<p>DOD Std 17</p> <p>DOD O-2000.12-H</p> <p>Strategic Goal 2I</p> <p>UFC 4-023-03</p>
<b>WEAPONS EFFECTS</b>		
Guidance to Assessors	Installation personnel can use weapon effects information for self-assessment, permitting prediction of weapons effects on people and structures and suggesting strategies to mitigate these effects. In addition, use of this data will raise awareness of weapons effects on people and structures.	

**FOR OFFICIAL USE ONLY**

<b>ILLUSTRATIVE TARGETS</b>		
Guidance to Assessors	Use available computer programs such as VAPO, BEEM, WINDAS, and HAZL to generate graphical representations of weapons effects. Prepare range-to-effect, weapons effects vulnerability radii, and iso-damage contours charts for illustrative targets based on the type and size weapon and tactic selected by the Terrorist Operations Specialist. Proposed mitigation measures, such as window hardening, facility upgrades, and effective barrier plans, should be included. 3-D graphics showing the effects of bomb attacks on buildings and people should be prepared to support Emergency Management consequence analysis. This data will be used to graphically illustrate response and effects that mitigation measures have on reducing damage and casualties.	
<b>TERRORIST INCIDENT RESPONSE (TIR) / TERRORIST CONSEQUENCE MANAGEMENT (TCM)</b>		
SE-PLN-09	<p><b>TIR / TCM Requirements:</b> The installation engineering staff should be tasked, prepared, and equipped to provide support to the installation’s response to a terrorist event. [Coordinate with Emergency Management.]</p> <ul style="list-style-type: none"> <li>• Are installation engineers part of the Emergency Operations Center (EOC) staff?</li> <li>• Have their roles and responsibilities been identified in the EOC Plan?</li> <li>• Are as-built drawings (latest designs / construction drawings / shop drawings, etc.) for all facilities available for use during an emergency? Are the drawings available in CAD or digital format?</li> <li>• Are engineers capable of, or is there an appropriate entity available to provide, structural analysis of incident sites in support of emergency responders and search and rescue operations?</li> <li>• Are installation engineers tasked, trained, and equipped to provide structural analysis of damaged buildings during consequence management operations?               <ul style="list-style-type: none"> <li>○ If not, is there a plan in place to procure such services?</li> </ul> </li> </ul>	<p>DOD Std 17, 20, 21</p> <p>DOD O-2000.12-H</p> <p>UFC 4-010-01 &amp; 4-010-02</p>
Guidance to Assessors	<ul style="list-style-type: none"> <li>• Perform structural analysis of buildings for immediate use.</li> <li>• Provide recommendations for the repair or demolition and renovation / rebuilding of damaged structures.</li> </ul>	

## FOR OFFICIAL USE ONLY

### PHYSICAL SECURITY MEASURES FOR SHIPS AND PORTS

Waterside security must include the establishment of a security perimeter at the water's edge to detect presence of terrorist threats. The security perimeter must be extended into the water if terrorists are assessed as having the capability to launch attacks using standoff weapons from boats or other craft. A security zone is established within the surveillance area extending from the high-water mark to a distance at least 3250 FT (1,000 M) from shore if possible. Barriers on the waterside of a DOD installation, facility, or asset afloat perform many basic functions performed on land, such as establishing boundary, isolating activity and discouraging visitors, and impeding passage by boat or swimmer. Several devices can be used to establish boundaries separating the DOD installation, facility, or asset from the surrounding or bordering waters. Among the devices that can be used to establish a boundary are buoys or floats, nets (where allowed), anchored or pile mounted navigation aids, and signaling devices. Log booms, blue barrels, 55-gallon drums, Dunlop, barges, gig-boats, whaleboats, and other small workboats at anchor and roving patrols by security boats.

FPCON Measure ALPHA 2. USN combatant ships, when in a non-U.S. Navy controlled port, deploy barriers to keep vehicles away from the ship if possible (100 feet in U.S. ports and 400 feet outside U.S. (minimum standoff distances)). For DOD non-combatants in a non-U.S. Government controlled port, request husband agent arrange and deploy barriers to keep vehicles away from the ship if possible (100 feet in U.S. ports and 400 feet outside U.S. (minimum standoff distances)).

FPCON Measure BRAVO 4. Restrict vehicle access to the pier. Discontinue parking on the pier. Consistent with local rules, regulations, and/or the SOFA, establish unloading zones and move all containers as far away from the ship as possible (recommend 100 feet in the United States, 400 feet outside the United States as the minimum stand-off distance).

Other FPCON Measures as applicable.

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

SE-PLN-PORT-01	<p><b>Waterside Physical Security System:</b> Should include barriers to establish a boundary, isolate activities, and impede passage by boat or swimmer. [Coordinate with Security Operations.]</p> <ul style="list-style-type: none"> <li>• Are waterside assets secured? <ul style="list-style-type: none"> <li>○ Is standoff provided IAW FPCON Measures?</li> <li>○ Is there a Barrier Plan for waterside security?</li> <li>○ What types of barriers are used?</li> <li>○ Do barriers prevent direct, unchallenged access onto piers, wharves, or docks when ships are moored?</li> <li>○ Do selected barriers provide surface and subsurface protection?</li> </ul> </li> </ul>	DOD Std 7  DOD O-2000.12-H
SE-PLN-PORT-02	<p>Effective exclusion zones (safety and security) should be contained in plans to establish appropriate standoff for ships in port, load out staging areas, and concentrations of personnel (passenger terminals and liberty ships). Exclusion zones may be established by water barriers (such as oil booms), buoys and signs, patrol boats, fencing, etc. [Coordinate with Security Operations.] Where parking is necessary on piers, wharves, or docks, it shall be limited to essential government or vetted commercial vehicles.</p> <ul style="list-style-type: none"> <li>• Are ACPs to piers, wharves, or docks designed and built to support access control procedures to ensure vehicles allowed access are controlled, vetted, and searched?</li> <li>• Do parking locations provide standoff IAW DOD criteria?</li> </ul>	DOD Std 7, 13  DOD O-2000.12-H
<b>PHYSICAL SECURITY MEASURES FOR AIRFIELDS</b>		
	<p><b>Airfields</b> represent special challenges because of the unique character of the facilities and the DOD assets they support. Engineers / Planners should consider the establishment of multiple internal security perimeters, hardening of selected buildings against terrorist attack, and hardening of MEVAs (petroleum storage, aircrew facilities, and maintenance facilities) and other facilities collocated on the installation. Engineers / Planners should be fully aware of DOD regulations and instructions, Service regulations and instructions, and COCOM requirements for enhanced physical security protection for many types of munitions stored at DOD airfields.</p>	
SE-PLN-AF-01	<p>The AT Plan shall include protection of airfields located on the installation. [Coordinate with Security Operations.]</p> <ul style="list-style-type: none"> <li>• Is standoff provided IAW FPCON Measures? <ul style="list-style-type: none"> <li>○ Do standoff considerations for airfield facilities, aircraft, equipment, and other assets afford an appropriate level of protection?</li> </ul> </li> </ul>	DOD Std 7  DOD O-2000.12-H

# FOR OFFICIAL USE ONLY

## Annex D Infrastructure Engineering Benchmarks

The installation's utilities infrastructure is assessed to determine reliability, survivability, and the installation's ability to respond and recover in the event of a terrorist or multi-hazard incident. Utilities infrastructure is critical for life sustainment, fire and life safety, and the operation of mission critical facilities and functions. Electrical and backup power systems support mission critical operations. Water systems support cooling systems, sanitary sewage disposal, firefighting systems, and industrial and potable water uses. Communications systems support mission critical voice and data systems. Bulk fuel storage and refueling is vital for air and fleet operations, installation support, emergency vehicles and equipment, and refuel of emergency generators. HVAC system shut down capability is critical in protection of personnel in the event of an airborne contaminant incident. Firefighting systems are critical for life and fire safety of personnel and mission critical facilities and operations. The assessment includes interviews and discussion with functional area experts; review of maps, plans, and documents; and site investigation of critical utility nodes.

Benchmarks below are followed by questions to help establish the interview process and obtain relevant information.

### 1. AT RISK MANAGEMENT

IE-RM-01	<p><b>Threat Assessment.</b> Installation commanders shall establish a Threat Assessment (TA) process to identify the full range of known or estimated terrorist capabilities or hazards for those personnel and assets for which they have AT responsibilities.</p> <ul style="list-style-type: none"><li>• Does the TA address all hazards approach for infrastructure supporting the installation's mission?</li><li>• Are threats to infrastructure and warnings disseminated to persons responsible for infrastructure protection?</li></ul>	<p>DOD Std 4</p> <p>JP 3-07.2, Ch. III, VI, &amp; AP B</p> <p>DOD O-2000.12-H, Chapter 5</p> <p>DOD O-2000.12-P,</p> <p>Strategic Goal 1E</p>
----------	---	---

**FOR OFFICIAL USE ONLY**

<p>IE-RM-02</p>	<p><b>Criticality Assessment.</b> Installation commanders shall establish a Criticality Assessment (CA) process to identify, classify, and prioritize mission-essential assets, resources, and personnel critical to DOD mission success.</p> <ul style="list-style-type: none"> <li>• Does the CA identify assets necessary for mission accomplishment, to include supporting infrastructure? <ul style="list-style-type: none"> <li>○ Are single points of failure identified for the installation infrastructure?</li> </ul> </li> <li>• Has the installation identified critical assets off the installation when there are no alternative or independent systems on the installation?</li> <li>• Does the CA address effect of loss (local and strategic), recoverability, mission functionality, substitutability, and reparability of installation assets and supporting infrastructure?</li> <li>• Does the impact of loss to include local and strategic missions?</li> <li>• Have mission essential / critical personnel been identified? (Personnel responsible for operation and maintenance of critical infrastructure.) <ul style="list-style-type: none"> <li>○ Is there a process for identification, recall, and response by critical personnel? [Coordinate with Security Operations.]</li> </ul> </li> <li>• Are offices responsible for infrastructure, e.g. PWD or CE, and the fire department aware of the priority on assets? <ul style="list-style-type: none"> <li>○ Has the infrastructure critical to DOD, but not necessarily important to the installation, been identified and included in the CA?</li> </ul> </li> <li>• Report any critical infrastructure that is not on the CA to the Terrorist Operations specialist.</li> </ul>	<p>DOD Std 5</p> <p>DOD O-2000.12-H, Chapter 6, 22</p> <p>Strategic Goal 1F</p>
<p>IE-RM-03</p>	<p><b>Vulnerability Assessment.</b> Installation commanders shall provide a Vulnerability Assessment (VA) process to provide vulnerability-based analysis of mission-critical assets, resources, and personnel critical to mission success that are susceptible to terrorist attack.</p> <ul style="list-style-type: none"> <li>• Is infrastructure addressed in the installation’s VA process? Includes VA of critical roads, bridges, sea and air ports, and staging / bed down areas. [Coordinate with Terrorist Operations.]</li> <li>• Are Public Works / BCE engineers assigned to the installation’s VA team? <ul style="list-style-type: none"> <li>○ Have the engineers been trained on how to conduct a VA?</li> <li>○ Is there specific methodology established for the assessment of infrastructure?</li> </ul> </li> <li>• Are infrastructure vulnerabilities entered into the Core Vulnerability Assessment Management Program (CVAMP) and tracked until mitigated?</li> <li>• Does the assessment assess the dependencies, vulnerabilities, and effects of the disruption or loss of critical assets or supporting infrastructures on their plans and operations?</li> <li>• Does the assessment address all hazards: terrorism, fire, wind, equipment failure, lightning, snow, ice, earthquake, etc.?</li> </ul>	<p>DOD Std 6</p> <p>DOD Memo 3 Jul 03 - Water Policy</p> <p>Strategic Goal 1G</p> <p>OPNAVINST 11300.6A 5500.14D</p> <p>NAVMC DIR 3500.86</p> <p>UFC 4-020-01</p>

**FOR OFFICIAL USE ONLY**

	<p><b>WATER SYSTEM VULNERABILITY ASSESSMENT (WSVA)</b></p> <ul style="list-style-type: none"> <li>• Has installation conducted a WSVA covering the following areas?             <ul style="list-style-type: none"> <li>○ Water system serving 25 or more DOD consumers</li> <li>○ CONUS water systems serving over 3300 consumers fall under EPA regulations.</li> <li>○ OCONUS water from local supplier needs WSVA</li> </ul> </li> <li>• Does the Water VA cover the following areas:             <ul style="list-style-type: none"> <li>○ Review of pipes and conveyances?</li> <li>○ Hydraulic capacity of system to provide sufficient fire flows and adequate system pressure?</li> <li>○ Physical barriers?</li> <li>○ Access control to well buildings on site, water treatment facilities, and water storage facilities?</li> <li>○ Water collection, treatment, and storage facilities?</li> <li>○ Automated systems used by water system?</li> <li>○ Use and handling of chemicals?</li> <li>○ O&amp;M of the system?</li> </ul> </li> <li>• What type water testing is being performed and at what intervals?</li> <li>• Can testing be varied according to threat?</li> <li>• Is the WSVA reviewed annually?</li> </ul>	
IE-RM-04	<p><b>Risk Assessment.</b> A risk assessment (RA) process shall be established for the installation and reviewed annually. It should include critical infrastructure and assets. [Coordinate with Terrorist Operations.]</p> <ul style="list-style-type: none"> <li>• Is the assessment used to justify physical security changes for protection of infrastructure (physical and cyber)?             <ul style="list-style-type: none"> <li>○ Is the DBT used when developing protective measures?</li> </ul> </li> <li>• Does the RA provide critical asset assurance analysis, planning, prioritization, resource programming, and response necessary to mitigate the disruption or loss of critical assets?</li> <li>• Can critical functions be transferred to alternate locations and resume operations quickly, without an unacceptable degradation to the mission?</li> <li>• Have protective / compensatory measures for critical infrastructure been developed?             <ul style="list-style-type: none"> <li>○ Have contingency plans been developed for the long term or temporary loss of the infrastructure?</li> </ul> </li> <li>• Have plans been developed by the owner / user for protection of critical infrastructure / infrastructure critical to mission accomplishment?</li> <li>• Have high risk vulnerabilities been mitigated or there plans in place to mitigate these vulnerabilities?</li> <li>• Are engineers included in the selection, design, and construction of physical countermeasures identified to reduce the risk?</li> <li>• Have compensatory measures been identified for all risks that are accepted?</li> <li>• Has a plan of action been developed to implement the countermeasures?</li> <li>• Has the assessment been translated into action items for either resourcing or procedural corrections?</li> <li>• Have waivers been requested when risk is accepted (if required)?</li> </ul>	<p>DOD Std 3</p> <p>JP 3-07.2, AP D1</p> <p>DOD O-2000.12-H, Chapter 8</p> <p>Strategic Goal 1H</p>

**FOR OFFICIAL USE ONLY**

IE-RM-05	<p>The fire chief or the authority having jurisdiction for the installation should prepare a fire risk management survey for the installation, to include each building or facility. This assessment should address the capability of the fire department to provide protection to the installation based on fire risk of buildings, location and grouping of buildings on the installation, use of buildings, and fire hazards in and around buildings.</p> <ul style="list-style-type: none"> <li>• Is chief aware of primary gathering and mission essential buildings?</li> <li>• Does the chief accomplish a fire risk survey IAW service guidance?</li> <li>• Has a fire risk assessment study been determined for the installation, to include each building?             <ul style="list-style-type: none"> <li>○ Are buildings rated according to risk?</li> <li>○ Has calculation of water supply been determined? How much water is available from water storage and alternate sources during emergency conditions? During a power outage?</li> </ul> </li> </ul>	<p>DOD Std 21</p> <p>DODI 6055.6, Encl. 2, Par 1.b and c</p> <p>AR 420-90, Chapter 6-5</p> <p>AFI 32-2001</p> <p>OPNAVINST 3440.17</p>
----------	--	--

**2. AT PLANNING**

2.A

**AT PLAN ELEMENTS**

IE-PLN-01	<p>The Installation Commander’s AT Plan must be a coordinated effort between the many AT planning and response elements of the installation based upon its organic capabilities.</p> <ul style="list-style-type: none"> <li>• Is infrastructure addressed in the AT Program / Plan?</li> <li>• Are critical missions prioritized for utility support?</li> <li>• Does the installation’s AT Plan contain the applicable AT Planning and Response elements based upon its organic capabilities, such as contingency plans, building restoration?</li> <li>• Resource support infrastructure function?</li> <li>• Public Works/BCE?</li> <li>• Are all installation tenants included in the AT Plan?</li> </ul>	<p>DOD Std 7</p> <p>DOD O-2000.12-H, Chapter 9, AP4</p> <p>Strategic Goal 2D</p>
-----------	---	--

**FOR OFFICIAL USE ONLY**

<p>IE-PLN-02</p>	<p>The Installation Commander shall develop and implement site-specific FPCON measures for the protection of infrastructure critical to mission accomplishment.</p> <ul style="list-style-type: none"> <li>• Was the threat assessment used to develop levels of protection for infrastructure?</li> <li>• Are measures in place to implement the following FPCON measures?             <ul style="list-style-type: none"> <li>○ FPCON Measure NORMAL 1: Are the infrastructure nodes secured and checked randomly?</li> <li>○ FPCON Measure NORMAL 2: Are the critical assets identified as supporting infrastructure?</li> <li>○ FPCON Measure BRAVO 2: Has the installation developed a plan to control access to critical infrastructure?</li> <li>○ FPCON Measure BRAVO 3: Have buildings housing critical infrastructure and exterior critical infrastructure (substations, etc.) been identified and provided protection against IED threats? Is obscuration provided for exterior equipment?</li> <li>○ FPCON Measure BRAVO 4: Have rooms containing infrastructure systems been secured?</li> <li>○ FPCON Measure BRAVO 8: Is there a process to conduct random inspections and testing of water?</li> <li>○ FPCON Measure BRAVO 10: Are there plans to enhance off-installation security of critical infrastructure at DOD facilities? Has coordination for additional security at off-installation infrastructure been conducted (non-DOD critical assets)?</li> <li>○ FPCON Measure CHARLIE 5: How does the installation verify the identity of individuals entering water storage and treatment facilities? Is there a list of authorized personnel?</li> <li>○ FPCON Measure CHARLIE 6: What is the plan to implement monitoring of chemical and biological agents in water supply? Is there a process to prevent unauthorized taps into facility water systems?</li> <li>○ FPCON Measure CHARLIE 7: What is the process / plan to protect all designated infrastructure critical to mission accomplishment? What are the procedures implemented by local / host-government authorities to protect off-installation critical infrastructure?</li> <li>○ FPCON Measure CHARLIE 8: Are patrols increased for critical infrastructure components?</li> <li>○ FPCON Measure CHARLIE 9: Is all infrastructure critical to mission protected and coordination made with local authorities?</li> </ul> </li> </ul>	<p>DOD Std 22</p> <p>DOD O-2000.12-H, Chapter 10</p> <p>Strategic Goal 2F</p>
<p>IE-PLN-03</p>	<p>Contracted services identified as essential to maintenance and restoration of critical assets and infrastructure should be included in acquisition planning to allow the services to continue in crisis situations.</p> <ul style="list-style-type: none"> <li>• Have services been identified that are so essential they must continue during a crisis situation?</li> <li>• Do plans address contractor access to base and critical facilities?</li> <li>• Do contingency plans require military members to replace contractor employees during a crisis or contingency?</li> </ul>	<p>DOD Std 18</p>

## FOR OFFICIAL USE ONLY

2.B	<b>INFRASTRUCTURE COLLOCATION</b>	
IE-PLN-04	<p>Critical infrastructure support elements should not be collocated to prevent or minimize multiple support systems from being destroyed simultaneously.</p> <ul style="list-style-type: none"> <li>• Are critical systems and nodes collocated?</li> <li>• Are facilities and habitat areas adequately separated from overhead high-voltage lines?</li> <li>• Are internal high-voltage feeder lines, branch circuit-distribution lines, and other power distribution equipment adequately separated from water and fuel storage tanks and pipes?</li> </ul>	DOD Std 19
IE-PLN-05	<p>Identify those key utility components susceptible to all-hazard damage</p> <ul style="list-style-type: none"> <li>• Are all system components identified? (i.e., component name, identification, wind speed, and/or duration limitations.)</li> <li>• Are there trees or other standing objects that are located close enough to system components that, if they fell, they would impact the distribution system?</li> <li>• Are key system components protected from electrical surge or lightning strike?</li> <li>• Are key system components protected from rain, water, or flooding effects?</li> <li>• Are key system components protected from heat and humidity (not fire) effects?</li> <li>• Are key system components resistant to cold and icing effects?</li> <li>• Are key system components protected from hail damage?</li> </ul>	DOD Std 19
2.C	<b>COMMUNICATIONS (Information Assurance)</b>	
IE-PLN-06	<p>Installations should develop a written contingency plan for communication outages. The plan should be integrated into and support the Terrorist Incident Response measures of the base. Provisions in this plan should not conflict with other provisions in the AT Plan.</p> <ul style="list-style-type: none"> <li>• Are the systems protected with passwords and firewalls, including modems and RF access?</li> <li>• Does the site maintain a plan that addresses continuous availability of communications systems supporting missions (i.e., COOP)?</li> <li>• Does the plan enlist external parties (i.e., commercial providers) (ensure external parties are listed in plans, and POCs and contact phone numbers are noted)?</li> <li>• Do these plans address issues of redundancy, survivability, reliability, and security?</li> <li>• Does the plan address issues of prioritization, system restoration, communications systems usage, and emergency operations and maintenance?</li> <li>• Have prioritization procedures been exercised to ensure that communications critical to executing EACH mission are not interrupted?</li> </ul>	DOD Std 20

## FOR OFFICIAL USE ONLY

IE-PLN-07	<p>The commercial communications cable route diagrams and interfaces affecting the installation are available to provide information for security, redundancy, and diversity.</p> <ul style="list-style-type: none"> <li>• Are cable diagrams and paths / routes as described in the documentation?</li> <li>• Are the drawings and diagrams available in CAD or digital format?</li> </ul>	<p>DOD Std 19</p> <p>Strategic Goal 3C</p>
IE-PLN-08	<p>Redundancy and diversity in communication systems should exist to avoid single point vulnerabilities.</p> <ul style="list-style-type: none"> <li>• Is there diversity in the media used (e.g. RF, SATCOM, fiber optic cable, copper cable, and laser)?</li> <li>• What systems are available?</li> <li>• Which systems are used the most?</li> <li>• What networks support the systems (e.g. NIPRNET, SIPRNET, JWICS, and DRSN)?</li> <li>• For activity cabling: <ul style="list-style-type: none"> <li>○ Is there diversity in the external routing?</li> <li>○ How many cable entry / exits points onto the installation?</li> <li>○ Is a loop or ring used and is the ring self-healing, path switched such that a single break at any point does not sever connectivity between any two nodes?</li> <li>○ If so, is there adequate separation in fibers or are they all in the same cable trench conduit or follow the same path?</li> <li>○ What is the separation distance?</li> <li>○ Is it sufficient to prevent a “backhoe” type incident?</li> <li>○ Is it sufficient to keep the cables from crossing on the same bridge?</li> <li>○ Is there physical diversity in the internal cable plant?</li> <li>○ How many cable entry/exit points into the facilities?</li> <li>○ How many telephone switches serve the installation?</li> <li>○ Are remote switches capable of independently handling telephonic traffic in case of an outage at the dial control office?</li> <li>○ Is there sufficient separation such to prevent a single event from severing both cable paths’ connectivity?</li> </ul> </li> <li>• Are telecommunications closets (TC) stacked or in close proximity? (Note: If the TCs are stacked, then the assessor must determine if appropriate measures are used to control spread of fire up and flow of water down. In facilities with all telecommunications on one level, often the closets are side-by-side, where fire or other events in one will impact the other.)</li> <li>• Are classified communications distributed in a Protected Distribution System (PDS)? Is PDS integrity maintained?</li> <li>• Is there more than one data processing, switching, routing, or distribution facility? If only one, what is the impact of its loss?</li> <li>• What is the security, fire protection, and utility requirements of communication facilities? (Work with other team members for this expertise.)</li> <li>• Are clean fire suppression systems used in communications and data processing facilities?</li> <li>• Is access to the communication facilities controlled and monitored?</li> <li>• How many commercial telecommunication providers-Points of Presence (POP) are on the installation? In the facility? (Note: more than one provider is preferred with diverse, physically separated entry / exits onto the installation. Even if multiple providers are not used / available, diverse,</li> </ul>	<p>DOD Std 19</p> <p>Strategic Goal 3C and 5E</p>

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

	<p>physically separated entry / exits onto the installation are required with connectivity to multiple, physically separated central offices.)</p>	
<p>IE-PLN-09</p>	<p>Dependencies on and support provided to other infrastructure and critical assets and/or the communications systems should be identified.</p> <ul style="list-style-type: none"> <li>• Are roads and/or bridges on or near the site used as corridors for communications transmission media, i.e. fiber optic or copper?</li> <li>• Do all mission-critical communications elements that rely on electric power have dedicated emergency generators?</li> <li>• Does the Dial Central Office (DCO), TCF, and/or the Main Communications Center / Information Technology Center have a dedicated emergency generator and/or uninterruptible power source (UPS) plant?</li> <li>• Are the emergency generators auto-start?</li> <li>• What are the emergency generators' fuel capacities (provide generator)? What is the fuel storage capacity? Are the generator fuel storage tanks normally kept full? How long will the generator operate on the normal available fuel supply? Is there a fuel source available to refill the tanks in emergency conditions?</li> <li>• Who is responsible for the maintenance of the HVAC systems? (Provide POC and name of organization.)</li> <li>• For HVAC systems that have been identified, is there a dependency on water?</li> <li>• Is the HVAC system used for mission essential equipment on backup power?</li> </ul>	
<p>IE-PLN-10</p>	<p>Computer controlled (DDC, DCS, or SCADA) utilities and mechanical systems shall be protected from unauthorized access by appropriate security measures.</p> <ul style="list-style-type: none"> <li>• Are the systems protected with passwords and firewalls, including modems and RF access?</li> <li>• Is the modem disconnected / turned off when not being utilized by authorized users?</li> <li>• Is DDC coordinated with shutdowns for SIP?</li> <li>• Are monitoring and control system protected (i.e., passwords, access controls, etc.) from unauthorized access such as open or public communications paths (i.e., Internet, phone line, or radio frequency)?</li> <li>• Are passwords restricted to authorized users on a need to have basis?</li> <li>• On what platform does this monitoring and control system operate?</li> <li>• What organization (address and contact number) designed, installed, and operates this monitoring and control system?</li> <li>• Does the site have onsite or offsite operational and/or maintenance personnel for the monitoring and/or control system? How many?</li> <li>• How often are this system's operational parameters checked or monitored?</li> <li>• Does the site maintain replacement components for this monitoring and control system or have appropriate contracts to ensure immediate response and repair?</li> </ul>	<p>DOD Std 19</p> <p>TSWG SCADA Ver 1.0</p>

**FOR OFFICIAL USE ONLY**

2.D	<b>POWER</b>	
IE-PLN-11	<p>The installation must identify and evaluate its source of electric power to determine whether there is adequate flexibility, reliability, and redundancy (i.e. load shedding capabilities, multiple feeders, looped system, multiple switches, etc) to provide primary power to critical assets.</p> <ul style="list-style-type: none"> <li>• What is the source of electrical power?</li> <li>• Are all hazards included in the evaluation of power reliability, such as natural disasters, including snow, ice, tornadoes, winds, floods, trees and vegetation, accidents, animals, earthquakes, etc.?</li> <li>• Do single points of failure (SPF) exist within the distribution system?</li> <li>• Is the power capacity adequate for installation demand level?</li> <li>• Are there redundant electrical feeds to the installation?</li> <li>• Are electrical feeds physically diverse?</li> <li>• Are the electrical distribution lines in a radial or looped pattern?</li> <li>• Are there switches to route the electric around a disruption or fault?</li> <li>• Who maintains the power distribution lines?</li> <li>• Is there a Commander-approved plan for load shedding? Is it automatic?</li> <li>• Do substation cross connects have sufficient capacity for required loads, or is a load study planned?</li> <li>• Are power outages recorded in a log for reference and history?</li> <li>• Are there frequent power outages? If so, what are the causes of outages?</li> <li>• How easily or quickly can power be restored?</li> <li>• Are there any spare transformers and other equipment?</li> <li>• Is there a priority power restoration plan?</li> </ul>	DOD Std 19

## FOR OFFICIAL USE ONLY

IE-PLN-12	<p>The installation should provide properly sized backup generators at critical facilities with enough capacity to support those facilities during prolonged periods of primary power outage (i.e. command and control centers, security desk, communication facilities, hospitals, fire department, life safety systems, computer systems, etc.) Backup power units should be maintained and tested on a regular basis.</p> <ul style="list-style-type: none"> <li>• Has a determination been made of what mission functions (what percentage) are not functional under generator power?</li> <li>• Are generators located at mission critical facilities and life safety locations?</li> <li>• Are portable generators available for emergencies?             <ul style="list-style-type: none"> <li>○ Where are they stored?</li> <li>○ At what facilities can they be used?</li> <li>○ Are the number and capacity of them adequate?</li> </ul> </li> <li>• Are generators regularly maintained and tested?             <ul style="list-style-type: none"> <li>○ Under actual load, load bank, or no load conditions?</li> <li>○ Does load bank have inductive load?</li> <li>○ What is frequency of testing?</li> </ul> </li> <li>• Do generators have an automatic transfer switch?             <ul style="list-style-type: none"> <li>○ If not, who will start generators and how long will this take?</li> </ul> </li> <li>• Are generators collocated with other essential equipment?</li> <li>• Is there a generator refueling matrix? Does it match the prioritization of mission-essential facilities?</li> <li>• Are fuel tanks for backup generators secured, along with piping to generators? Are tanks of sufficient size to support an extended outage? Are the tanks normally kept full? How long will generators operate on the normally available fuel supply?</li> <li>• What level of security is provided for the generators? Fenced? DOD approved padlocked gate? Barbed wire? Lighted? Bollards? Locked generator cabinet doors?</li> <li>• Are tanks locked or placed inside a locked facility to prevent contamination and potential ignition?</li> <li>• If above ground, are tanks double walled and/or have spill containment (dike) that will prevent a running fire?</li> </ul>	<p>DOD Std 19 AFI 32-1063 NFPA 101</p>
IE-PLN-13	<p>Installations should develop a written contingency plan for power outages. The plan should be integrated into and support the Terrorist Incident Response measures of the base. Provisions in this plan should not conflict with other provisions in the AT Plan.</p> <ul style="list-style-type: none"> <li>• Does the power contingency plan address elements such as:             <ul style="list-style-type: none"> <li>○ Description of system, locations</li> <li>○ Mission priorities</li> <li>○ Single line diagram</li> <li>○ Essential personnel, names, phone numbers</li> <li>○ Generators installed, locations, size, fuel capacity</li> <li>○ Portable generators, pre-designated</li> <li>○ Uninterruptible Power Supply (UPS)</li> <li>○ Automatic Transfer Switch (ATS)</li> <li>○ Is there a generator refueling matrix? Does it match the prioritization of mission-essential facilities?</li> </ul> </li> </ul>	<p>DOD Std 20 AFI 10-24 AFI 10-211</p>

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

IE-PLN-14	<p>The location of the primary power source should be evaluated from the critical mission or primary gathering buildings out to at least the first connection to a commercial supply grid past a single point of failure. Single points of failure in this system should be evaluated for physical security measures and ability to reconstitute the node if damaged.</p> <ul style="list-style-type: none"> <li>• Where are critical nodes in the system?</li> <li>• What level of security is provided to substations and other equipment? Is it commensurate with the location? Fenced? Barbed wire? DOD approved padlocked gates? Inside a secure and sturdy building? Is obscuration provided for exterior equipment?</li> <li>• Are facilities housing these activities vulnerable to attack by virtue of their location or quality of their construction?</li> </ul>	DOD Std 19
IE-PLN-15	<p>The installation should provide Uninterruptible Power Supplies (UPS) to data processing equipment or computers at critical facilities, with enough capacity to support the equipment and sufficient duration to maintain operation until generator or commercial power is restored.</p> <ul style="list-style-type: none"> <li>• Is there sufficient back-up power (UPS) to support required equipment in case of a primary power outage? How long can the computer equipment continue to operate on the power from the UPS system?</li> <li>• Is a UPS providing continuous backup power during power interruptions?</li> <li>• Are batteries properly maintained?</li> <li>• Is the UPS room kept at temperature storage requirements for batteries? (77°F optimal for gel cell)</li> <li>• Are battery rooms secured, ventilated, and/or alarmed?</li> <li>• Are the CCTV cameras and monitors, IDS alarm systems, and security force radios also provided with backup power (UPS and generator)?</li> </ul>	DOD Std 19
IE-PLN-16	<p>Access Control Points should have backup power for electronic equipment, and active vehicle barriers to sustain an extended primary power outage. Computers should also have a UPS in addition to backup power. [Coordinate with Security Operations]</p> <ul style="list-style-type: none"> <li>• Is there a backup power system for the ACP?</li> <li>• Is lighting within 100' of the ACP also on this backup power?</li> <li>• Do computer processors used for screening or security also have a UPS?</li> </ul>	DOD Std 19 UFC 4-022-01

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

2.E	<b>WATER DISTRIBUTION AND SUPPLY</b>	
IE-PLN-17	<p>Water systems should have the capability to meet current water needs of critical assets (capacity, redundancy, reliability, etc.)</p> <ul style="list-style-type: none"> <li>• What type of contract does the site have with the water distribution provider?</li> <li>• Is the water distribution system looped? Are there multiple dead ends?</li> <li>• Is water supplied through multiple sources which are supplied from diverse locations? Can the systems back feed one another?</li> <li>• How does the age and condition of the water distribution system affect its reliability and ability to supply water for fire suppression?</li> <li>• Does the site have an emergency provisions contract with the provider?</li> <li>• Where are the points of connection to the external water system and flow capacity?</li> <li>• Are water distribution systems looped to prevent dead ends in system?</li> <li>• What is the site's average water usage (gallons per day)? (Summer and winter, if significantly different.)</li> <li>• How much water is required for critical mission accomplishment (gallons per day)? (Summer and winter, if significantly different.)</li> <li>• Does the water system meet supply demands of potable, industrial, and fire-fighting water to support the critical mission?</li> <li>• Does the site's backup capability provide an adequate supply of potable, industrial, and fire-fighting water to support the critical mission?</li> <li>• How long (hours or days) will the site's storage capability sustain the demands for water during critical mission accomplishment?</li> <li>• What is the operating pressure range of the network?</li> <li>• How is the water pressure maintained?</li> <li>• Does the site have backup or auxiliary pumps to maintain network pressure?</li> <li>• Does the site have backflow prevention devices?</li> <li>• Has the site experienced disruptions to water service, or have any significant events occurred in the past that affected water service?</li> <li>• Are there sufficient onsite personnel to operate the water system during crisis or high demand (i.e., natural disaster, heightened threat, or system disruption), to include essential personnel designated to enter the site?</li> <li>• What chemical treatments (chemical types) are used in providing water to the site, and where are they stored? Is the water supply chlorinated?</li> <li>• Is the water supply tested regularly for contaminants?</li> <li>• Are chemicals properly and safely stored and are MSDS available?</li> <li>• Does the system share rights-of-ways with other infrastructures?</li> </ul> <p><b>SECURITY</b> (Coordinate with Security Operations.)</p> <ul style="list-style-type: none"> <li>• Are treatment plants locked and secured to prevent unauthorized access?</li> <li>• Is the treatment plant staffed 24/7?</li> <li>• Is a chain of custody established with the suppliers?</li> <li>• Is the treatment plant monitored 24 hours a day? Who monitors? Who responds?</li> <li>• Do treatment plants, water storage tanks, and water towers have the necessary lighting, cameras, intrusion detection systems, or alarms to provide adequate monitoring?</li> </ul>	DOD Std 7

## FOR OFFICIAL USE ONLY

IE-PLN-18	<p>Documents will be maintained detailing the current configuration of the water distribution system supporting critical assets.</p> <ul style="list-style-type: none"> <li>• Does the site maintain current drawings, blueprints, maps, schematics, timetables, line drawings, and photographs of water system key assets? <ul style="list-style-type: none"> <li>○ Are Geographical Information System (GIS) or Computer-aided Design (CAD) formats available?</li> <li>○ What date was the last revision of the items identified?</li> </ul> </li> <li>• Has this information been protected, not been made available to the public, and kept in a secure onsite location?</li> </ul>	DOD Std 19
IE-PLN-19	<p>Installations should develop a written contingency plan for water outages. The plan should be integrated into and support the Terrorist Incident Response measures of the base. Provisions in this plan should not conflict with other provisions in the AT Plan.</p> <ul style="list-style-type: none"> <li>• Does the water contingency plan address elements such as: <ul style="list-style-type: none"> <li>○ Site water distribution maps, isolation valves?</li> <li>○ Essential personnel, names, phone numbers?</li> <li>○ Spare parts?</li> <li>○ POC for water containers, bottled water, vendors?</li> <li>○ Water curtailment plan, priority?</li> <li>○ Plan for public notices?</li> <li>○ Fire department alternate water source?</li> </ul> </li> </ul>	DOD Std 21  DOD Memo 3 Jul 03 Water Policy  AFI 10-21  AFI 10-211
2.F	<b>FIRE PROTECTION</b>	
IE-PLN-20	<p>The fire communications center should be adequately equipped with appropriate fire alarm monitoring, communication, and recording devices. This equipment includes all fire reporting telephone circuits, direct lines, and the intra-base radio master control. Procedures for operation, response, maintenance and administration of the systems should be provided.</p> <ul style="list-style-type: none"> <li>• Is there a central fire communications center? <ul style="list-style-type: none"> <li>○ Is there a backup fire control center?</li> </ul> </li> <li>• Is the fire communications center adequately equipped with appropriate fire alarm monitoring, communication, and recording devices?</li> <li>• Are the alarms transmitted by radio or over copper/fiber lines?</li> <li>• Do the lines pass through a single point of failure?</li> </ul>	DOD Std 20 UFC 3-600-01 NFPA 101
IE-PLN-21	<p>Equipment in mission critical facilities should have fire protection to protect equipment critical nodes and minimize damage. These facilities may include telephone switch rooms, SIPRNET and SIPRNET hubs, satellite links, and alarm panels.</p> <ul style="list-style-type: none"> <li>• Is a wet-pipe sprinkler system provided?</li> <li>• Is power disconnected upon activation of sprinkler system, including all UPS systems?</li> <li>• Is there a smoke evacuation system?</li> <li>• Is a supplementary clean agent suppression system, approved by the authority having jurisdiction, used as a first response to fire?</li> <li>• Is handheld clean agent fire suppression equipment adequate in respect to location and type?</li> </ul>	DOD Std 21  AF ETL 02-15  3-600-01 NFPA 101

**FOR OFFICIAL USE ONLY**

IE-PLN-22	<p>Installations should establish and maintain a fire inspection program. This program should be integrated into and support the AT Plan of the installation and should not conflict with other provisions in the plan.</p> <ul style="list-style-type: none"> <li>• Do the buildings have fire evacuation plans / escapes routes, emergency lighting, and exits? Are the fire evacuation plans posted in conspicuous locations in the building? Do the fire evacuation plans reflect the current building layout?</li> <li>• Does the installation have a written fire prevention plan?</li> <li>• What are the fire training, drills, and fire awareness programs?</li> <li>• Is there a sufficient number of fire inspectors?</li> <li>• Is the fire department included in the design review process?</li> <li>• Are life-safety systems (panic hardware, exit lights, emergency lights, fire extinguishers, and stairs) installed, maintained, inspected, and functioning?</li> <li>• Are existing buildings, new construction, and major renovation projects in compliance with life safety code requirements?</li> <li>• Are fire-protection systems (sprinkler or suppression systems) installed and maintained in buildings according to the fire-safety codes?</li> <li>• Are fire hydrants inspected and maintained adequately? Who performs these functions?</li> <li>• When used as an auxiliary water source, approved by the AHJ, do fire hydrants have backflow preventers or fire department locks?</li> <li>• Are fire-alarm systems installed and maintained in buildings according to NFPA fire-safety codes?</li> <li>• Do fire detection and suppression systems transmit an alarm to the fire communications center?</li> <li>• What is the heat / smoke detection and alarm capability?</li> <li>• How is it maintained? Tested?</li> <li>• What are the building smoke-evacuation capabilities?</li> </ul>	<p>DOD Std 21</p> <p>DODI 6055.6</p> <p>NFPA 101</p> <p>UFC 3-600-01</p>
2.G	<b>BULK FUELS</b>	
IE-PLN-23	<p>The storage of bulk fuel tanks and fuel distribution systems should consider location on installation, safe distance from other facilities, fire suppression capability, and fuel truck parking.</p> <ul style="list-style-type: none"> <li>• Is the fuel storage area easily accessible by fire equipment? <ul style="list-style-type: none"> <li>○ Is the storage area adequately separated from primary gathering buildings and mission critical buildings?</li> </ul> </li> <li>• Can fuel be supplied from bulk storage during power failures?</li> <li>• Do tanks have a floating roof?</li> <li>• Do tanks have a piping system for application of aqueous film forming foam (AFFF)?</li> </ul>	<p>DOD Std 19</p>

## FOR OFFICIAL USE ONLY

IE-PLN-24	<p>The fuel system should meet the identified needs of critical assets.</p> <ul style="list-style-type: none"> <li>• List the consumption and storage (days of supply) requirements (by type).</li> <li>• What types of petroleum products and their quantities are available at the site?</li> <li>• Who are the fuel distributors serving the site? (Identify company name, company address, and types of fuel provided.)</li> <li>• Who are the fuel distributors' points of contact (POCs)? (Office name and telephone numbers.)</li> <li>• What are the site's contracted quantities of fuel by the fuel distributor? (Name and contracted quantity for distribution, volume, type of product, frequency of delivery, and contract timeframes.)</li> <li>• How is the fuel delivered to the site (i.e., pipeline, tanker, barge, tanker truck, or railcar)?</li> <li>• Does the installation have an alternate delivery plan? Has the plan been tested?</li> <li>• What is the fuel distributors' priority of petroleum service to this site compared with other petroleum customers? (Those customers the petroleum distributors place ahead of the site (i.e., hospitals or residential customers, etc.))</li> <li>• Can berms, if required, around storage tanks contain 110% of fuel tank storage? Or are tanks double-walled?</li> </ul>	DOD Std 19
IE-PLN-25	<p>Installations should develop a written contingency plan for loss of fuel. The plan should be integrated into and support the Terrorist Incident Response measures of the base. Provisions in this plan should not conflict with other provisions in the AT Plan.</p> <ul style="list-style-type: none"> <li>• Does the fuel contingency plan address elements such as: <ul style="list-style-type: none"> <li>○ Description of system, locations?</li> <li>○ Mission priorities?</li> <li>○ Essential personnel, names, phone numbers?</li> <li>○ Agreements with alternate fuel suppliers?</li> </ul> </li> </ul>	DOD Std 20
IE-PLN-26	<p>The location of the fuel source should be evaluated for ability to distribute fuel during utility outages to critical mission or high-occupancy buildings. Single points of failure in this system should be evaluated for physical security measures and ability to reconstitute the node if damaged.</p> <ul style="list-style-type: none"> <li>• Where are critical nodes in the system?</li> <li>• Is there positive control of fuel delivery and storage on the installation?</li> <li>• What level of security is provided to equipment? Is it commensurate with the location? Fenced? Barbed wire? Padlocked gates? Inside a secure and sturdy building?</li> <li>• Are facilities housing these activities vulnerable to attack by virtue of their location or quality of their construction?</li> </ul>	DOD Std 19
IE-PLN-27	<p>Compressed gases susceptible to explosion or which support combustion should have appropriate standoff from buildings and flammable material.</p> <ul style="list-style-type: none"> <li>• Are the fuel containers properly stored and secured?</li> <li>• Are storage tanks properly grounded?</li> </ul>	DOD Std 19 DOD 6055.9

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

2.H	CBRN	
IE-PLN-28	<p>Installation personnel should review all new construction and major renovation projects to ensure Chemical, Biological, Radiological, and Nuclear (CBRN) protective measures are addressed.</p> <ul style="list-style-type: none"> <li>• Has the installation developed a CBRN DBT including TIC/TIM threats? [Coordinate with EM team member.]</li> <li>• Are CBRN protective measures addressed in the review of new construction and major renovation projects? (Especially in regard to HVAC outside air intakes and mailrooms.)</li> <li>• Are new construction and major renovations designed to accommodate future addition of CBRN protective measures if not presently justified?</li> </ul>	<p>DOD Std 17 DODI 2000.18 Strategic Goal 4E UFC 4-010-01 UFC 4-024-01</p>
IE-PLN-29	<p>Inhabited buildings, primary gathering, and mission critical facilities shall have a method to automatically close the outside air intake or procedures to manually shut down the HVAC system when contaminants are detected. For complex building situations, refer to UFC.</p> <ul style="list-style-type: none"> <li>• Does each facility maintain a plan to shut down the HVAC following a CBRN/TIC/TIM incident? Would this be done manually, automatically, or centrally from an electronic Energy Management Control System?</li> <li>• Are all vents, e.g. kitchen and bathroom, shut off during HVAC shutdown?</li> <li>• Is the plan incorporated into a mass notification plan? (See EM benchmarks.)</li> <li>• Are CBRN detectors in operation? If so, what individuals are trained to operate the equipment? What is the CBRN detection architecture?</li> <li>• Do written procedures exist for HVAC shutdown for both internal and external events with procedures for evacuations or sheltering in place?</li> </ul>	<p>DOD Std 21 Strategic Goal 4E UFC 4-010-01, Standard 18 UFC 4-024-01</p>
IE-PLN-30	<p>The need to establish collective protection for critical and essential personnel and mission critical facilities and the required level of protection should be determined based on mission criticality and ability to relocate, reconstitute, or delay the mission taking place in the facility.</p> <ul style="list-style-type: none"> <li>• Mission critical facilities should be included in a CBRNE risk management process (based on CBR threat, criticality, and vulnerability) to determine appropriate level of protection for mission critical and essential personnel. [See Annex E, Emergency Operations.] <ul style="list-style-type: none"> <li>○ Are CBR threats considered for mission critical facilities?</li> </ul> </li> <li>• Is the level of protection based on CBR threat?</li> <li>• Would any attempt to interrupt or contaminate the HVAC delivery be detected by the site?</li> <li>• Have HVAC system operators and maintenance personnel practiced or exercised operations in CBRN environments within the past 12 months?</li> <li>• Are toxic industrial chemicals transported (by road, rail, ship, etc) or stored near or upwind of the installation?</li> <li>• Can the HVAC system supporting a critical mission or asset operate independently if this monitoring and/or control system is not operational?</li> <li>• Is the HVAC system designed so no SPFs exist in paths linking system elements deemed critical to the operations of a network? (With this design, two or more simultaneous failures or errors must occur at the same time to cause a service interruption.)</li> <li>• Does the existing HVAC system have a filtration system for CBRN agents? Is the system designed to remove particulate (biological, radiological, nuclear) and/or gaseous (chemical) agents? Is the system properly maintained and regularly tested?</li> </ul>	<p>DOD Std 21 FEMA 452 AFI 10-211 UFC 4-024-01</p>

## FOR OFFICIAL USE ONLY

IE-PLN-31	<p>Outside air intakes for HVAC systems, especially ones servicing mission critical rooms and facilities or inhabited buildings and primary gathering facilities, should be located at least three meters (10 ft) above ground level. The height rule is required for inhabited buildings and primary gathering facilities designed / constructed after FY2002.</p> <ul style="list-style-type: none"> <li>• Is the HVAC system of each building susceptible to attack?</li> <li>• Does the HVAC system have some type of fresh-air intake?</li> <li>• What is the ease of access to HVAC equipment?</li> <li>• Is the HVAC equipment below ground with an exterior air intake shaft?</li> <li>• Are all mechanical room doors kept locked?</li> <li>• Is the HVAC equipment on the ground on the exterior of building?</li> <li>• Is the HVAC equipment located at the second floor or higher with access through exterior wall or on the roof of building? If so, is there an exterior ladder to wall access or roof? Is the ladder secured to prevent unauthorized access?</li> <li>• Is the HVAC system for the mail room isolated from the rest of the building to prevent a CBR release in the room from spreading to adjacent areas? Is the envelope (walls, floor, and ceiling) around the mail room well sealed?</li> <li>• Is the HVAC system for the publicly accessible areas of the building (lobbies, loading docks, cafeterias, etc.) isolated from the rest of the building to prevent a CBR release in the areas from spreading to adjacent areas? Is the envelope (walls, floor, and ceiling) around these areas well sealed?</li> <li>• Is the building well sealed to prevent a CBR agent released outside from being drawn into the building by natural infiltration?</li> <li>• Are packages, mail, and supplies being brought into the building screened for potential CBRN agents?</li> </ul>	<p>DOD Std 17 UFC 4-010-01 UFC 4-024-01</p>
IE-PLN-32	<p>Chlorine gas containers (and other hazardous gas containers), such as those used at water treatment facilities and swimming pools, should have sufficient physical security with leak detection. An alarm should transmit to a security or fire department alarm panel that is monitored at all times.</p> <ul style="list-style-type: none"> <li>• Is chlorine gas stored in vicinity of primary gathering or mission essential buildings?</li> </ul>	DOD Std 21
<b>3. RESOURCE APPLICATION</b>		
IE-RA-01	<p>The DOD component shall submit prioritized, unfunded AT requirements (to include those submitted or considered for Cbt-RIF) to the Joint Staff J-3 DD AT/HD, J34 on an annual basis pursuant to current DOD Program Objective Memorandum (POM) guidance and timelines using the Core Vulnerability Assessment Management Program (CVAMP) or a Service version of VAMP.</p> <ul style="list-style-type: none"> <li>• Is all critical infrastructure vulnerability assessment data included in CVAMP (HHQ and local)?</li> <li>• Are critical infrastructure vulnerabilities tracked until mitigated?</li> <li>• Have unfunded requirements been identified to mitigate infrastructure vulnerabilities?</li> <li>• Have major and high-risk vulnerabilities been mitigated through funding decisions, improved security TTPs, or risk reduced to a lower acceptable level? [Requires thorough review of vulnerability assessment documents.]</li> </ul>	<p>DOD Std 30 Strategic Goal 4D</p>

**FOR OFFICIAL USE ONLY**

**Annex E  
Emergency Management Benchmarks**

<b>1. AT RISK MANAGEMENT</b>		
	<p>Risk management is a comprehensive process and a critical planning element of the Installation Emergency Management (IEM) Program. The risk management process shall be performed by the IEM Working Group (IEMWG) under the authority of the Installation Commander. The completion of the risk management process will occur prior to the development of the initial IEM Plan or IEM Plan update and will be an on-going process that informs the annual review and update of the IEM Plan. Effective risk management requires support of Emergency Management (EM), Public Works, Security, Information Technology, Logistics, Intelligence, Medical, Fire, and Emergency Services (F&amp;ES) and, as appropriate, local, state, tribal, other Military Service(s), or host-nation (HN) partners in the local community. The all-hazards risk assessment shall identify and monitor hazards and threats and the likelihood of their occurrence, the vulnerability of the installation, and the consequences of those hazards and threats.</p> <p>Each assessment below shall be conducted and validated annually prior to the update or review of the IEM Plan. The results of the assessments should determine the basis and justification for IEM Program enhancements, program planning, and budget requests. Developed risk management methodologies must consist of, at a minimum, the following types of assessments:</p>	<p><b>DODI 6055.dd</b></p> <p>DODI Std 3 DODI 2000.16</p>
EM-RM-01	<p><b>HAZARD / THREAT ASSESSMENT (HA / TA)</b> [Formerly titled the CBRNE TA.] DOD, command, or unit-level evaluation (assessment) to identify hazards and associated risks to person, property, and structures and to improve protection</p>	<p><b>DODI 6055.dd</b></p> <p>DOD Std 4</p>

**FOR OFFICIAL USE ONLY**

	<p>from natural or manmade disasters or hazards. HAs serve as one of the foundational components for effective EM activities, including planning, resource management, capability development, public education, and training and exercises.</p> <ul style="list-style-type: none"> <li>• Has a HA / TA been conducted by the IEMWG? (The IEMWG is the EM equivalent of the existing AT Working Group and is responsible for ensuring the activities associated with establishing the IEM Program on their respective DOD installation.)             <ul style="list-style-type: none"> <li>○ Does this assessment address all-hazards based on relevancy / applicability and take into consideration those hazards identified in DODI 6055.dd, <i>DOD Installation Emergency Management Program</i>, Enclosure 4, Appendix 2?</li> </ul> </li> <li>• Does the HA / TA:             <ul style="list-style-type: none"> <li>○ Identify and characterize the hazards? (Determine if the installation is susceptible to natural disasters (hurricanes, tornadoes, and earthquakes), major accidents (aircraft, industrial), or terrorist attacks and what additional hazards they pose.)</li> <li>○ Evaluate each hazard for severity and frequency? (Determine how often these hazards affect the installation and what actions may help reduce their severity.)</li> <li>○ Estimate the impact of the hazard and/or threat? (Identify what missions or areas are potentially affected by these hazards (consider special events.))</li> <li>○ Identify risk reduction opportunities? (This step takes mitigation actions to reduce the threat or impact of the hazard.)</li> <li>○ Address the potential threat of terrorist use of CBRNE weapons?</li> <li>○ Incorporate the respective Combatant Command's (COCOM) WMD/CBRNE Threat Assessment?</li> <li>○ Identify state and non-State actors' CBRNE capability status summary?</li> <li>○ Identify the toxic industrial chemicals (TIC) and toxic industrial materials (TIM) located on the installation and local community? (This must identify the specific hazard ID, quantity, and location.)</li> <li>○ Identify facilities and transportation modes having the potential of releasing TIC / TIMs (accidental or intentional) that could impact the installation. (Areas to consider are TIC/TIM manufacturing / using facilities, refineries, railroads, highways, POL tank farms, nuclear power plants, ship yards, etc.)                 <ul style="list-style-type: none"> <li>▪ Coordinate with the Local Emergency Planning Committee (LEPC) to identify the type and location of TIC/TIMs that could affect the installation following an accidental or intentional release</li> <li>▪ LEPC link: <a href="http://yosemite.epa.gov/oswer/lepcdb.nsf/HomePage?openForm">http://yosemite.epa.gov/oswer/lepcdb.nsf/HomePage?openForm</a> (Only for CONUS installations.)</li> </ul> </li> </ul> </li> <li>• Has the IEMWG:             <ul style="list-style-type: none"> <li>○ Coordinated with the installation Threat Working Group (TWG) to analyze installation local Threat Assessments?</li> <li>○ Considered the full range of known or estimated terrorist capabilities and possibilities of non-hostile incidents?</li> <li>○ Integrated threat information prepared by the intelligence community in liaison with federal, state, and local law enforcement?</li> </ul> </li> </ul>	<p>DODI 2000.16</p> <p>DODI 2000.18 Guideline 8</p> <p>Strategic Goal 1E</p>
--	---	--

**FOR OFFICIAL USE ONLY**

<p>EM-RM-02</p>	<p><b>VULNERABILITY ASSESSMENT (VA)</b>  All installations shall perform a VA. This type of VA should address the broad range of hazards and threats, including CBRNE, to the installation and its personnel as identified in the HA / TA.</p> <ul style="list-style-type: none"> <li>• Has the installation conducted an annual VA and documented the results?</li> <li>• Was the All-Hazards VA Template used to conduct the VA and document the results? (Not mandatory, but highly suggested.)</li> <li>• Does the VA: <ul style="list-style-type: none"> <li>○ Consider the range of identified and projected response capabilities necessary for responding to any type of hazard identified by the local or COCOM HA / TA?</li> <li>○ Address the adequacy of installation AT / IEM / CBRNE plans, standard operating procedures (SOP), checklists, etc?</li> <li>○ Identify appropriate courses of action to address vulnerabilities and solutions for enhanced protection of DOD personnel and resources?</li> <li>○ Include identified defense industrial base and Defense Critical Infrastructure Program (DCIP) assets?</li> <li>○ Identify potentially exploited vulnerabilities and suggest options for eliminating or mitigating the exploitation of those vulnerabilities?</li> <li>○ Provide a vulnerability-based analysis of the installation’s critical assets? Identify potentially exploited vulnerabilities and suggest options for eliminating or mitigating the exploitation of those vulnerabilities?</li> </ul> </li> </ul>	<p>DOD Std 6  DODI  2000.16</p> <p>DODI  2000.18  Guideline 1  &amp; 8</p> <p>DODI  6055.dd</p> <p>Strategic  Goal 1G</p>
<p>EM-RM-03</p>	<p><b>FOOD VULNERABILITY ASSESSMENT (FVA)</b></p> <ul style="list-style-type: none"> <li>• Has a Food Defense Program been implemented by the Installation Commander?</li> <li>• Has an office of primary responsibility (OPR) been identified for the installation?</li> <li>• Has a multi-disciplinary Food Defense Assessment Team (FDAT) (or equivalent) been established to conduct systematic reviews and assessments of the installation’s food systems IAW US Army Technical Guide (TG) 188, <i>US Army Food and Water Vulnerability Assessment Guide</i>; US Air Force Instruction (AFI) 10-246, <i>Food and Water Protection Program</i>; or other COCOM or Service guidance?</li> <li>• Has an annual FVA been conducted IAW applicable COCOM and Service guidance?</li> <li>• Does the FVA identify potential vulnerabilities for each agency’s facilities that store, prepare, serve, and/or sell food, ice, or bottled water, including schools, child care centers, exchange operations, contract operations, recreation facilities, etc?</li> <li>• Have Food Defense AT measures been incorporated into the logistical and contracting processes for establishments on or off the installation that supply, transport, store, prepare, serve, and/or sell food, ice, or bottled water to the installation?</li> <li>• Are procedures established for increasing surveillance during higher Force Protection Conditions (FPCON) or increased threat?</li> </ul>	<p>DOD Std 6  DODI  2000.16</p> <p>Combatant  Command  (COCOM)  AT and  Service  Guidance</p> <p>Strategic  Goal 1G</p>

**FOR OFFICIAL USE ONLY**

EM-RM-04	<p><b>CAPABILITY ASSESSMENT</b></p> <ul style="list-style-type: none"> <li>• Has the installation conducted a Capability Assessment? (Should consider contingency planning activities.)</li> <li>• Does the assessment:             <ul style="list-style-type: none"> <li>○ List installation resources by type to provide asset visibility, to include external capabilities?</li> <li>○ Identify resources provided by the local community and/or host-nation?</li> <li>○ Determine the costs of the direct and indirect effects of the identified hazards?</li> </ul> </li> <li>• Has the Installation Emergency Manager complied with requirements of Personnel Categorization? [See EM-PLN-27]</li> <li>• Was the VA referenced to assist with the Capability Assessment?</li> </ul>	DODI 6055.dd
<b>2. AT PLANNING</b>		
EM-PLN-01	<p><b>INSTALLATION EMERGENCY MANAGER</b></p> <ul style="list-style-type: none"> <li>• Has the Installation Commander designated, in writing, an Installation Emergency Manager responsible for all IEM Program functions at their assigned level?</li> <li>• Does the installation Emergency Manager employ resource management activities to coordinate the prioritization and allocation of resources at the installation? Resource management activities include development of resource management objectives that address:             <ul style="list-style-type: none"> <li>○ Personnel, equipment, training, facilities, funding, expert knowledge, materials, technology, information, intelligence, and the timeframe within which they are needed.</li> <li>○ Quantity, response time, capability, limitations, cost, and liability connected with using the resources.</li> <li>○ Resources and partnership arrangements essential to the IEM Program (e.g., MAAs, MOUs, MOAs).</li> <li>○ Implementation of resource management procedures to locate, acquire, store, distribute, maintain, test, and account for personnel, services, resources, materials, and facilities procured or donated to the IEM Program. These procedures shall address, at a minimum, the following resource management tasks:                 <ul style="list-style-type: none"> <li>▪ Establishing processes for describing, requesting, tracking, and taking inventory of resources.</li> <li>▪ Activating these processes prior to and during an incident.</li> <li>▪ Dispatching resources prior to and during an incident.</li> <li>▪ Deactivating or recalling resources during or after an incident.</li> <li>▪ Establishing contingency planning for shortfalls of resources in accordance with National Fire Protection Association (NFPA) 1600.</li> <li>▪ Develop and maintain the IEM Plan.</li> <li>▪ Collaborate and coordinate with local, state, tribal, other Military Service(s) and host-nation emergency managers to achieve the highest possible level of IEM Plan integration and interoperability.</li> </ul> </li> </ul> </li> <li>• Does the Installation Emergency Manager attend Local Emergency Planning Committee (LEPC) meetings regularly?</li> </ul>	DODI 6055.dd  NFPA Standard 1600

**FOR OFFICIAL USE ONLY**

<p>EM-PLN-02</p>	<p><b>INSTALLATION EMERGENCY MANAGEMENT WORKING GROUP (IEMWG)</b></p> <ul style="list-style-type: none"> <li>• Has the Installation Commander established an IEMWG responsible for ensuring the activities associated with establishing an IEM Program on their respective DOD installation?</li> <li>• Has the IEMWG developed a written charter and included it in the IEM Plan? <ul style="list-style-type: none"> <li>○ Does the charter identify composition, responsibilities, meeting frequency, etc?</li> </ul> </li> <li>• Does the IEMWG meet quarterly, at a minimum? <ul style="list-style-type: none"> <li>○ Are meeting minutes accomplished and maintained for at least two years?</li> </ul> </li> <li>• Does the composition of the IEMWG include, at a minimum, the following: <ul style="list-style-type: none"> <li>○ Installation Commander or Commander’s representative?</li> <li>○ Installation Emergency Manager?</li> <li>○ F&amp;ES representative?</li> <li>○ Medical and Public Health representative?</li> <li>○ Security representative?</li> <li>○ Logistics representative?</li> <li>○ Communications representative?</li> <li>○ Public Affairs representative?</li> <li>○ Tenant and subordinate command and unit representative?</li> <li>○ Representation from existing working groups (e.g., TWG, ATWG, and, where appropriate, local, state, tribal, other Military Service(s), and host-nation response partners in the local community)?</li> </ul> </li> <li>• Has the IEMWG conducted a Hazard / Threat, Capability, and Vulnerability Assessment?</li> </ul>	<p>DODI 6055.dd</p>
<p>EM-PLN-03</p>	<p><b>INSTALLATION EMERGENCY MANAGEMENT (IEM) PLAN</b></p> <ul style="list-style-type: none"> <li>• Has the installation developed an IEM Plan designed to support pre-incident planning and mitigation activities; emergency response, medical, and public health needs; equipment needs; law enforcement; training; intelligence support; security; and recovery?</li> <li>• Is the IEM Plan flexible enough for use in all emergencies, including unforeseen events, yet detailed enough to provide a course of action for Installation Commanders to proceed with preplanned responses to an unexpected event?</li> <li>• Has the installation adopted and implemented National Response Framework (NRF) and National Incident Management System (NIMS) policies and guidance into the IEM Plan? <ul style="list-style-type: none"> <li>○ Are these procedures consistent with the NIMS and the Incident Command System (ICS) for all DOD domestic installations? (See DEPSECDEF Memo “Implementation of the National Response Plan and National Incident Management System,” dated 29 Nov 2005)</li> <li>○ To the extent possible, do OCONUS installations consider using NRF and NIMS principles when implementing their IEM programs?</li> </ul> </li> <li>• Are procedures established for civil authorities to request immediate support under imminently serious conditions IAW DODD 3025.1? (Immediate response may be necessary to save lives, prevent human suffering, or mitigate great property damage.)</li> </ul>	<p>DODI 6055.dd</p>

## FOR OFFICIAL USE ONLY

	<p><b>IEM Plan Elements</b></p> <ul style="list-style-type: none"><li>• Does the IEM Plan assign responsibilities to organizations and individuals and is it designed to support areas of pre-incident planning, emergency response, medical and public health needs, equipment, law enforcement, training, intelligence support, security, response, and recovery?</li><li>• Is the IEM Plan coordinated with other protection-related program plans to include, but not be limited to, AT, Physical Security, Fire &amp; Emergency Services, HAZMAT, etc?</li><li>• Is the IEM Plan updated annually and does it incorporate lessons learned and opportunities for improvement identified during exercises and risk management activities?</li><li>• Does the IEM Plan address the following, at a minimum:<ul style="list-style-type: none"><li>○ Mission, goals, and objectives of the IEM Program?</li><li>○ Functional roles, responsibilities of, and lines of authority for all personnel, organizations, and agencies assigned EM and response responsibilities?</li><li>○ Preparedness activities, to include:<ul style="list-style-type: none"><li>▪ Risk Management?</li><li>▪ Prevention planning that establishes interim and long-term actions to reduce and/or eliminate identified hazards and/or threats to the installation?</li><li>▪ Mitigation planning that establishes interim and long-term actions to reduce the impact of hazards and/or threats that cannot be eliminated?</li><li>▪ Training?</li><li>▪ Exercises?</li><li>▪ Interagency coordination?</li><li>▪ Equipment?</li></ul></li><li>○ Response planning that establishes response actions and assigns responsibilities for carrying out specific emergency response actions? Specific response planning considerations include:<ul style="list-style-type: none"><li>▪ Continuity of operations planning that identifies mission essential personnel, procedures, and resources as well as contact information of stakeholders to be notified, critical and time-sensitive applications, alternative work sites, processes, and functions that shall be maintained while the installation is recovering.</li><li>▪ Evacuation management and mass care planning that addresses mass care concept, family assistance, sheltering-in-place, local and remote safe haven, civilian shelter, personnel accountability, special needs management, and animal needs management.</li></ul></li><li>○ Volunteer and donations management procedures been established for organizing and coordinating the receipt of unsolicited services and/or goods in a manner that does not interfere with ongoing response and recovery efforts?</li><li>○ Recovery planning that provides short-term and long-term priorities for restoration of functions, services, resources, facilities, programs, and infrastructure?</li><li>○ Communications through all phases of an emergency that address communications capabilities and operation of major communications nodes such as dispatch centers, mobile command posts, incident</li></ul></li></ul>	
--	---	--

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

	<p>command vehicles, and 911 services, with recording capability for each installation, either direct support (government owned and operated) or in general support from another organization.</p> <p><b>IEM Plan Structure</b></p> <ul style="list-style-type: none"> <li>• Does the plan address these three phases of incident management per the NRF: prepare, respond, and recover?</li> </ul>	
EM-PLN-04	<p><b>ALL-HAZARDS INCIDENT RESPONSE PLANNING</b></p> <p>Develop all-hazards incident response measures consistent with DOD Directive 2000.12, established criteria, or guidance, and include these measures in the overall IEM Plan. The measures shall include procedures for determining the nature and scope of an all-hazard incident response; procedures for coordinating Security, F&amp;ES, Medical, HAZMAT, and other emergency responder capabilities; and steps to recover from the incident while continuing essential operations. Each installation response occurs under different circumstances and involves different response actions. Installations must rely on their own resources; Mutual Aid Agreements (MAA); Status of Forces Agreements (SOFA); and federal, state, local, non-governmental organizations (NGO), and host-nation resources and capabilities to respond.</p> <ul style="list-style-type: none"> <li>• Has the installation developed all-hazards incident response measures and included them in the IEM Plan?</li> <li>• Do measures include procedures for determining nature and scope of incident response and procedures for coordinating F&amp;ES, security, medical, and EOD emergency responders, etc?</li> <li>• Do procedures address bomb threats, hostage situations, anti-hijacking, assassinations, vehicle-borne improvised explosive devices (VBIED), etc.?</li> <li>• Are procedures established to permit critical or emergency-essential personnel entry onto the installation during increased FPCONs? (Consider installation/local emergency responders and vehicles, medical providers, emergency operations center staff, etc.)</li> </ul>	DODI 6055.dd

**FOR OFFICIAL USE ONLY**

<p>EM-PLN-05</p>	<p><b>CBRNE INCIDENT RESPONSE PLANNING</b></p> <ul style="list-style-type: none"> <li>• Has a CBRNE Incident Response Annex to the IEM Plan been developed that integrates facilities, equipment, training, personnel, and procedures into a comprehensive effort to provide appropriate protection to personnel and critical missions on the installation? (May be a stand alone plan or annex to the IEM Plan.)</li> <li>• Does the annex/plan contain detailed procedures that first and emergency responders must follow for responding to CBRNE incidents?</li> <li>• Have detailed SOPs been developed by each agency tasked to support the annex/plan? (F&amp;ES, Security Forces, medical, Explosive Ordnance Disposal, Public Affairs, local community responders, etc.)</li> <li>• Does the annex/plan identify who is responsible for sampling, packaging, and chain of custody of CBRNE materials?             <ul style="list-style-type: none"> <li>○ Do procedures describe who, what, when, where, and how these processes are conducted?</li> <li>○ Are personnel trained and certified to conduct these operations?</li> </ul> </li> <li>• Does the annex/plan contain search procedures for secondary devices?             <ul style="list-style-type: none"> <li>○ Has EOD coordinated/approved search procedures?</li> </ul> </li> <li>• Are plume modeling procedures developed?             <ul style="list-style-type: none"> <li>○ Do procedures describe who, what, when, where, and how plume modeling is conducted?</li> <li>○ Do procedures describe how the most current weather data is provided to the Incident Commander?</li> </ul> </li> <li>• Is the installation aware of the reach-back capability to request plume modeling through DTRA's Operations Center at             <ul style="list-style-type: none"> <li>○ Comm: (703) 767-2118</li> <li>○ DSN: 427-2118</li> </ul> </li> <li>• Is the list of TIC / TIMs identified in the HA / TA referenced in the annex/plan?</li> <li>• Does the F&amp;ES and Emergency Operations Center (EOC) possess a current copy of the HA / TA?</li> <li>• Are procedures developed to implement site-specific CBRNE preparedness and emergency response measures that are synchronized with a corresponding FPCON level?</li> <li>• Are procedures developed for requesting contract clean-up / restoration crew after a HAZMAT or CBRN event?</li> <li>• Does the annex / plan address security and/or possible evacuation of DOD personnel and their dependents located OCONUS (Noncombatant Evacuation Operations (NEO))? (May be addressed in a separate plan.)</li> <li>• Does the Installation Emergency Manager maintain a current inventory of all emergency response equipment on the installation as well as what is available via mutual aid assistance through local communities or host-nation?</li> <li>• Has the installation received emergency response equipment through the Guardian Installation Protection Program (PPE, detection equipment, decontamination equipment, mass notification system, etc.)?             <ul style="list-style-type: none"> <li>○ Is this equipment included in the installation emergency response equipment inventory list?</li> <li>○ Is equipment utilized, secured and accounted for, shelf-life tracked, available for immediate use, and maintained and inspected?</li> </ul> </li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p>DODI 2000.18, Guideline 2 &amp; 4</p> <p>DOD O- 2000.12-H, Ch. 11</p> <p>Strategic Goal 2D</p> <p>National Response Framework (NRF)</p>
------------------	--	---

**FOR OFFICIAL USE ONLY**

<p>EM-PLN-06</p>	<p><b>MASS WARNING AND NOTIFICATION SYSTEM PLANNING</b></p> <ul style="list-style-type: none"> <li>• Has the installation developed a mass warning and notification system capable of warning all personnel within 10 minutes of incident notification at the dispatch center?</li> <li>• Does the system meet the criteria contained in the Unified Facilities Criteria (UFC) 4-021-01, <i>Design and O&amp;M: Mass Notification Systems</i>?</li> <li>• Does the installation use the types of mass warning and notification system described in the UFC e.g., Individual Building System, Giant Voice, and Telephone Alerting System?             <ul style="list-style-type: none"> <li>○ Does the installation use other redundant systems to conduct mass notification i.e., local area network, Commander’s access channel, radios, bullhorns, etc.?</li> </ul> </li> <li>• Is each system used by the installation addressed in the Communications Annex to the IEM Plan?             <ul style="list-style-type: none"> <li>○ Does guidance describe who, what, when, where, and how each system is activated, maintained, and tested?</li> </ul> </li> <li>• Do all new inhabited buildings possess a mass warning and notification system as required by UFC 4-02-01?             <ul style="list-style-type: none"> <li>○ <u>Inhabited buildings</u> are buildings or portions of buildings routinely occupied by 11 or more DOD personnel and with a population density of one person per 40 gross square meters (430 gross square feet)</li> </ul> </li> <li>• Do all new primary gathering buildings possess a mass warning and notification system?             <ul style="list-style-type: none"> <li>○ <u>Primary gathering buildings</u> are inhabited buildings routinely occupied by 50 or more DOD personnel</li> </ul> </li> <li>• Do all new billeting buildings possess a mass warning and notification system capability?             <ul style="list-style-type: none"> <li>○ <u>Billeting</u> is any building or portion of a building, regardless of population density, where 11 or more unaccompanied DOD personnel are routinely housed, including Temporary Lodging Facilities and military housing permanently converted to unaccompanied housing.</li> </ul> </li> <li>• Is the mass warning and notifications system tested regularly, unless restricted by local or host-nation ordinances?</li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p><b>DODI 6055.dd</b></p> <p>UFC 4-021-01</p> <p>Strategic Goal 2I</p>
------------------	---	--

**FOR OFFICIAL USE ONLY**

<p>EM-PLN-07</p> <p align="center"><b>Will be addressed in future IA Annex Benchmarks</b></p>	<p><b>COMMUNICATIONS PLANNING</b></p> <ul style="list-style-type: none"> <li>• Does the installation have a well-defined Communication Plan that includes the capability to communicate within the DOD, with personnel engaged in the response, and with civil authorities?</li> <li>• Is this a stand-alone plan or annex to the IEM Plan?</li> <li>• Does the annex/plan address:             <ul style="list-style-type: none"> <li>○ Communication capabilities, redundancies, and limitations?</li> <li>○ Installation mass warning and notification systems?</li> <li>○ 911 services?</li> <li>○ Dispatch center?</li> <li>○ Incident command vehicles, mobile command post?</li> <li>○ Land mobile radio (LMR) systems used by first responders and interoperability with local community?</li> <li>○ Location of radio repeaters, identification of dead spots not covered by LMRs, and workarounds for emergencies in such areas?</li> </ul> </li> <li>• Do installation first responders (Security, F&amp;ES, Medical, EOD, etc.) have adequate LMR communications?             <ul style="list-style-type: none"> <li>○ Can installation first responders communicate effectively between each other and local community responders via LMRs?                 <ul style="list-style-type: none"> <li>▪ What work-around methods are used when LMRs are not interoperable?</li> </ul> </li> <li>○ Do LMRs provide adequate coverage on the installation?                 <ul style="list-style-type: none"> <li>▪ Have dead spots been identified?</li> <li>▪ Are radios on a trunked system?</li> <li>▪ Are radios capable of secure communications?</li> </ul> </li> </ul> </li> <li>• Is the system narrow-band compliant?</li> </ul>	<p>DOD Std 21 DODI 20001.6</p> <p>DODI 2000.18, Guideline 6</p> <p>Strategic Goal 2G, 2I</p>
---	--	--

## FOR OFFICIAL USE ONLY

<p>EM-PLN-08</p>	<p><b>EVACUATION AND SHELTER-IN-PLACE (SIP) PLANNING</b></p> <p>SIP is a means to provide low-cost, short-term protection against the effects of CBRNE agents or the accidental or deliberate release of TIC/TIMs. The purpose of SIP is to make a shelter out of the place you are in and protecting yourself until help arrives. SIP is only for a short duration, roughly two to three hours or less.</p> <ul style="list-style-type: none"> <li>• Is evacuation and SIP guidance included in the IEM Plan? <ul style="list-style-type: none"> <li>○ Do procedures describe who, what, when, where, and how both evacuation and SIP are conducted?</li> <li>○ Do procedures describe the mass warning and notification systems used to conduct evacuations and SIP?</li> <li>○ Are evacuation / SIP scenarios included in IEM exercises?</li> </ul> </li> <li>• Have SIP procedures been developed and tailored for each facility on the installation designated for SIP?</li> <li>• Do these procedures address: <ul style="list-style-type: none"> <li>○ Identifying and computing space required for SIP? (Should be on an upper floor, possess no windows, provide a communications capability, and be accessible during duty hours at a central location.)</li> <li>○ Preparing, maintaining, and location of SIP kits?</li> <li>○ Shutting down the heating, ventilation, and air-conditioning (HVAC) systems, exhaust fans, etc.?</li> <li>○ Closing / taping windows / doors?</li> <li>○ Training facility personnel to conduct SIP?</li> <li>○ Disseminating SIP announcements throughout the facility?</li> </ul> </li> <li>• Is evacuation and SIP guidance provided to installation personnel and housing residents?</li> <li>• Can the installation warn its resident population in affected areas of CBRNE hazard identification immediately, but no longer than 10 minutes after detection? (Warnings must include instructions to evacuate or SIP.) <ul style="list-style-type: none"> <li>○ Do procedures identify who is authorized to issue evacuation or SIP instructions i.e., Commander, F&amp;ES, Security Forces, etc.?</li> </ul> </li> </ul> <p>NOTE: The following sources provide excellent SIP guidance:</p> <ul style="list-style-type: none"> <li>• Multiservice Tactics, Techniques, and Procedures for Installation CBRNE Defense (FM 3-11.34), page 126.</li> <li>• <a href="http://www.nicsinfo.org/SIP%20Center.htm">http://www.nicsinfo.org/SIP%20Center.htm</a></li> <li>• <a href="http://www.securitymanagement.com/article/emergency-preparedness-gimme-shelter">http://www.securitymanagement.com/article/emergency-preparedness-gimme-shelter</a></li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p><b>DODI 6055.dd</b></p> <p>Strategic Goal 2D, 3F</p>
<p>EM-PLN-09</p>	<p><b>MEMORANDUM OF AGREEMENT/UNDERSTANDING (MOA/MOU) AND MUTUAL AID AGREEMENT (MAA)</b></p> <ul style="list-style-type: none"> <li>• Have MOU / MOA / MAAs been established with the local community or host-nation to ensure response capabilities are integrated into the IEM Plan, AT Plan, and Medical Response Plan?</li> <li>• Are MOU / MOA / MAAs reviewed annually and modified when and where appropriate?</li> <li>• Is there a POC who maintains and tracks all AT / IEM related MOU / MOA / MAAs for the installation?</li> <li>• Has the installation legal office reviewed all MOU / MOA / MAAs?</li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p>DODI 2000.18, Guideline 2</p> <p><b>DODI 6055.dd</b></p> <p>Strategic Goal 2H</p>

**FOR OFFICIAL USE ONLY**

<p>EM-PLN-10</p>	<p><b>FORCE PROTECTION CONDITIONS (FPCON)</b>                  Installation commanders shall establish policies and procedures for setting FPCON levels, FPCON transition, dissemination and implementation of FPCON measures, notification of higher headquarters and affected DOD Component headquarters, development of site-specific FPCON measures, and a waiver (exceptions) process for FPCON implementation (approved waivers shall be in writing, consistent with the guidelines outlined in DOD O-2000.12-H).</p> <ul style="list-style-type: none"> <li>• Has specific guidance been developed to implement the following FPCON measures on the installation?                     <ul style="list-style-type: none"> <li>○ Measure ALPHA 5: Initiate food and water operational risk management procedures, brief personnel on food and water security procedures, and report any unusual activities.</li> <li>○ Measure ALPHA 6: Test mass notification system.</li> <li>○ Measure BRAVO 8: Randomly inspect food and water for evidence of tampering or contamination before use by DOD personnel. Inspections should include delivery vehicles, storage areas, and storage containers.</li> <li>○ Measure CHARLIE 5: Ensure or verify the identity of all individuals entering food and water storage and distribution centers, use sign-in and sign-out logs at access control and entry points, and limit or inspect all personal items.</li> <li>○ Measure CHARLIE 6: Initiate contingency monitoring for chemical, biological, and radiological contamination as required. Suspend contractors and off-facility users from tapping into the facility water system. An alternate locally developed measure should be implemented when contractors are responsible for DOD water supplies or when water is provided by local (non-DOD) sources or agencies.</li> <li>○ Measure DELTA 13: Begin continuous monitoring for chemical, biological, and radiological contamination.</li> </ul> </li> </ul>	<p>DOD Std 22                  DODI                  2000.16</p> <p><b>DODI                  6055.dd</b></p> <p>Strategic                  Goal 2D</p>
------------------	---	--

**FOR OFFICIAL USE ONLY**

<p>EM-PLN-11</p> <p><b>Will be addressed in future IA Annex Benchmarks</b></p>	<p><b>INFORMATION OPERATIONS CONDITION (INFOCON)</b></p> <ul style="list-style-type: none"> <li>• Has an INFOCON program been implemented by the Installation Commander?</li> <li>• Is the program based entirely on higher command direction, or does the activity have supplemental local procedures?</li> <li>• Is Tailored Readiness Options (TRO) for specific incidents included in these procedures (e.g. virus/worm incident)?</li> <li>• Do local levels always remain at least as high as the DOD level?</li> <li>• Is there an effective training and certification program for INFOCON to ensure the activity can meet internal and external requirements (e.g. global exercises)?</li> <li>• Does the Commander periodically raise the INFOCON levels to ensure INFOCON implementers (system and network managers) are trained and procedures tested?</li> <li>• Does the installation use the DEFCON scale (note: CDRUSSTRATCOM directed by 27 Apr 06)?</li> <li>• Does the Commander establish exit criteria when INFOCON levels are raised?             <ul style="list-style-type: none"> <li>○ Have supporting commanders, services, and agencies developed MOAs that pre-coordinate INFOCON procedures and TROs with the supported combatant commander? (Also applies in host/tenant and cross network domain situations.)</li> </ul> </li> </ul>	<p>DOD Std 19 DODI 2000.16</p> <p>Strategic Command Directive 527-1</p>
--	--	---

## FOR OFFICIAL USE ONLY

EM-PLN-12	<p><b>MEDICAL RESPONSE PLANNING</b></p> <ul style="list-style-type: none"> <li>• Has the installation developed a Medical Response Plan?</li> <li>• Does the plan clearly describe how emergency responders and receivers from the installation, local community, or host nation conduct coordinated responses to all-hazards incidents?</li> <li>• Is the plan current, exercised, and signed by the Installation Commander?</li> <li>• Does the plan address:             <ul style="list-style-type: none"> <li>○ Incident command and organization of responders?</li> <li>○ Recall procedures?</li> <li>○ What constitutes a MASCAL incident for the installation: 2, 4, 6, personnel?</li> <li>○ Medical facility capabilities for the installation, local community, or host-nation? (Level of care, specialty, bed space, etc.)</li> <li>○ Installation medical team duties, responsibilities, and composition?</li> <li>○ Installation medical control center (MCC) operations?</li> <li>○ Communications capabilities (radios, cell phones, etc.) and interoperability with responders?</li> <li>○ Response after duty hours when medical facility is closed or minimally manned?</li> <li>○ MASCAL flow diagram?</li> <li>○ Securing the installation medical facility following a CBRNE incident?</li> <li>○ Bomb threat, evacuation, and shelter-in-place procedures?</li> <li>○ Resources available to provide first response, triage, transportation, casualty classification and tracking, and personnel accounting?</li> <li>○ MASCAL training and exercise requirements?</li> <li>○ Medical surveillance for illness resulting from a biological agent?</li> <li>○ Number of ground and air-ambulances available from installation, local community, or host-nation to support a MASCAL incident?</li> <li>○ Medical care equipment carried by medical personnel responding to the MASCAL, i.e., airway management bag, oxygen delivery system, trauma bag, ALS medication bag?</li> <li>○ Mortuary affairs functions, including fatality management and contaminated casualty and/or remains handling, decontamination, transportation, and temporary storage?</li> </ul> </li> <li>• Are Mutual Aid Agreements (MAA) established with the local community or host-nation medical facilities and are they current?</li> <li>• Does the public health or medical functional area designee:             <ul style="list-style-type: none"> <li>○ Direct and support inspections and investigations of suspected sources of health threats?</li> <li>○ Prioritize health surveillance activities and make force health recommendations?</li> <li>○ Coordinate Public Health Emergency Management resources to perform inspection and surveillance activities?</li> <li>○ Identify and direct compliance of applicable laws, policies, and implementation procedures governing dissemination of information?</li> <li>○ Conduct investigations and analyze results for health threats?</li> <li>○ Perform increased surveillance and disease investigations based on how much higher the disease and non-battle injury rates are compared to the reference (local) standards?</li> <li>○ Recommend health control measures based upon investigations?</li> </ul> </li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p>DODI 2000.18, Guideline 3</p> <p style="color: red;">DODI 6055.dd</p> <p>Strategic Goal 2D, 2G</p>
-----------	---	--

**FOR OFFICIAL USE ONLY**

	<ul style="list-style-type: none"> <li>• Has a Mass Prophylaxis Plan been developed for ensuring the distribution of medical countermeasures during a public health emergency?</li> </ul>	
EM-PLN-13	<p><b>DEFENSE CONTINUITY PROGRAM (DCP) AND PLAN</b></p> <p>Installation commanders shall have a comprehensive and effective DCP that ensures DOD Component Mission Essential Functions (MEF) continue under all circumstances across the spectrum of threats IAW Executive Order 12656 and Implementation Guidance on National Security Policy Directions on Enduring Constitutional Government and Continuity of Government Operations. Develop, coordinate, and maintain continuity plans and validate, update, and reissue plans every two years or more frequently as changes warrant.</p> <ul style="list-style-type: none"> <li>• Has a DCP and Plan been developed? (Continuity of Operations (COOP) for some Services.)</li> <li>• Has the installation identified and prioritized its organizational Mission Essential Functions (MEF)? (A MEF is the specified or implied tasks required to be performed by, or derived from, statute or Executive order and those organizational activities that must be performed under all circumstances to achieve DOD Component missions or responsibilities in a continuity threat or event. Failure to perform or sustain these functions would significantly impact DOD’s ability to provide vital services or exercise authority, direction, and control.)</li> <li>• Does the DCP / COOP Plan:             <ul style="list-style-type: none"> <li>○ Provide guidance to continue MEFs within 12 hours and be capable of sustaining MEFs for up to 30 days?</li> <li>○ Define emergency delegations of authority and orders of succession for key positions; identify and provide for alert / notification, movement, and training of continuity staffs; and address information technology and communications support to continuity operations?</li> <li>○ Identify relocation sites or platforms for component use during continuity threats or events? Site selection should consider geographical dispersion and maximum collocation and dual-use facilities.</li> <li>○ Provide for identification, storage, protection, and availability for use at relocation sites the vital records, material, and databases required to execute MEF?</li> <li>○ Outline a decision process for determining appropriate actions in implementing continuity plans and procedures with or without warning, during duty and non-duty hours, and address the stand-down of continuity operations and transition back to normal operations?</li> <li>○ Ensure that continuity programs are adequately planned, programmed, and budgeted, and that DCP-unique requirements are specifically identified in their budgets?</li> <li>○ Integrate continuity-related functions and activities into operations and exercises to assure that MEF can be performed across the spectrum of continuity threats or events?</li> </ul> </li> <li>• Has the DCP/COOP Plan been tested and exercised at least annually or as otherwise directed to evaluate readiness?</li> </ul>	<p>DOD Std 19</p> <p>DODD 3020.26</p> <p>DODI 3020.42</p> <p><b>DODI 6055.dd</b></p> <p>Federal Preparedness Circular 65</p>

## FOR OFFICIAL USE ONLY

EM-PLN-14	<p><b>CRITICAL ASSETS</b></p> <ul style="list-style-type: none"> <li>• Has the installation identified its critical assets that are vital to the successful accomplishment of the IEM Program following an all-hazards incident? (Critical assets are described in DOD 2000.16, Std 3 and DOD O-2000.12-H.)</li> <li>• Do these critical assets qualify as Mission Essential Functions (MEF) as described in DODD 3020.26, Defense Continuity Program (DCP)?             <ul style="list-style-type: none"> <li>○ If designated a MEF, is it included in the installation DCP/COOP Plan?</li> </ul> </li> <li>• If the critical asset is a facility, are shelter-in-place (SIP) procedures developed and tailored to the facility?             <ul style="list-style-type: none"> <li>○ Do SIP checklists provide adequate guidance to facility occupants (i.e., shutdown HVAC system and exhaust fans, close/tape windows and doors, relocate to higher floors or interior windowless room, etc.)?</li> <li>○ Are supplies available to conduct SIP (tape, plastic, towels, etc.)?</li> </ul> </li> <li>• Are procedures developed for conducting mass warning and notification for facility occupants?             <ul style="list-style-type: none"> <li>○ Are occupants familiar with the procedures?</li> <li>○ Are procedures exercised?</li> </ul> </li> <li>• Do emergency response vehicles have adequate access to the facility?</li> <li>• Are procedures established to permit access for emergency responders during FPCON CHARLIE and DELTA?</li> </ul>	<p>DOD Std 19 DODI 2000.16</p> <p>DOD O- 2000.12-H, C1.4.1.15</p> <p>DODD 3020.26</p> <p>UFC 4-021- 01</p>
EM-PLN-15	<p><b>EMERGENCY OPERATIONS CENTER (EOC)</b></p> <p>EOCs represent the physical location at which the coordination of information and resources to support the Incident Commander occur. The EOC is activated to support on-scene response during an escalating incident by relieving the burden of external coordination and securing additional resources. The EOC consists of personnel and equipment appropriate for the level of incident and can manage multiple incidents and planned events.</p> <ul style="list-style-type: none"> <li>• Has the installation designated a primary and alternate EOC?</li> <li>• Does the EOC use a common operating picture and information management system in order to execute and support actions listed in the IEM Plan and facilitate coordination of incident information?</li> <li>• Is the EOC operational 24/7 or activated when the situation dictates?             <ul style="list-style-type: none"> <li>○ Can the EOC be activated quickly and staffed if not manned 24/7?</li> </ul> </li> <li>• Has an EOC Plan been developed?</li> <li>• Are Emergency Support Functions (ESF) developed as described in the NRF? (ESFs are groupings of capabilities that provides the support, resources, program implementation, and services that are most likely needed during emergency response. They are the operational-level mechanism that provides support during an incident.)             <ul style="list-style-type: none"> <li>○ Are offices of primary responsibility (OPR) assigned to each ESF?</li> </ul> </li> <li>• Does the EOC Plan address:             <ul style="list-style-type: none"> <li>○ Activation, layout, and setup procedures?</li> <li>○ Recall procedures?</li> <li>○ Emergency notification rosters of appropriate agencies?</li> <li>○ Staff duties and responsibilities?</li> <li>○ Higher headquarters (HHQ) reporting procedures?</li> <li>○ BLUE DART reporting procedures?</li> <li>○ Communication capabilities and procedures?</li> <li>○ Resource dispatch and tracking?</li> </ul> </li> </ul>	<p>DOD Std 20 DODI 2000.16</p> <p><b>DODI 6055.dd</b></p> <p>Strategic Goal 2D</p>

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

	<ul style="list-style-type: none"><li>○ Compatibility / interoperability with local community emergency responders?</li><li>○ Equipment, supplies, and sustainability requirements for the primary and alternate EOC?</li><li>○ Relocation / evacuation procedures?</li><li>○ Security procedures (entry authorizations list)?</li><li>○ Coordination considerations with local community / other agencies?</li><li>● Are the following plans / checklists / SOPs maintained in the EOC, if applicable:<ul style="list-style-type: none"><li>○ Installation Emergency Management Plan?</li><li>○ AT Plan?</li><li>○ Defense Continuity Program Plan?</li><li>○ Medical Response Plan?</li><li>○ Bomb Threat Plan?</li><li>○ Evacuation / Shelter-in-Place Plan?</li><li>○ Barrier Plan?</li><li>○ Infrastructure Contingency Response Plans (water, electrical, sewage, etc.)?</li><li>○ Suspected Aircraft Theft / Anti-hijack Plan?</li><li>○ Hostage Situation Plan?</li><li>○ Civil Disturbance / Riot Control Plan?</li><li>○ Respective COCOM AT Operations Order?</li></ul></li><li>● Does the EOC possess adequate communications?<ul style="list-style-type: none"><li>○ Secure and non-secure telephones</li><li>○ Secret Internet Protocol Router Network (SIPRNet) and Non-secure Internet Protocol Router Network (NIPRNet)</li><li>○ Radio base station and/or land-mobile radios</li><li>○ Compatibility / interoperability with installation and local emergency responders</li><li>○ Secure and non-secure fax</li><li>○ Operational control of the installation mass warning and notification system</li><li>○ Television (commander's access channel, news, etc.)</li></ul></li><li>● Are command and control lines of communication established with HHQ and local / State EOCs?</li><li>● Are installation grid maps posted, current, and accurate?<ul style="list-style-type: none"><li>○ Is the same scale grid map used by all emergency responders?</li></ul></li><li>● Are activation and evacuation exercises conducted by EOC personnel?</li><li>● Are procedures established for monitoring incident development?</li><li>● Are procedures established to request WMD Civil Support Team (CST) assistance?</li></ul>	
--	---	--

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

<p>EM-PLN-16</p>	<p><b>FIRE AND EMERGENCY SERVICES (F&amp;ES) INCIDENT RESPONSE</b></p> <ul style="list-style-type: none"> <li>• Does F&amp;ES standard operating procedures (SOP) for CBRNE/hazardous material (HAZMAT) response address:             <ul style="list-style-type: none"> <li>○ Establishing command, control, and communications (C3) consistent with the NIMS and ICS?</li> <li>○ Personnel accountability?</li> <li>○ Fire suppression and search and rescue?</li> <li>○ Initial medical triage?</li> <li>○ Decontamination of ambulatory and non-ambulatory casualties?</li> <li>○ Preserving scene and evidence?</li> <li>○ Chain of custody documentation?</li> <li>○ Recovery and reconstitution?</li> </ul> </li> <li>• What HAZMAT/CBRNE response capability level does the installation F&amp;ES provide, Offensive or Defensive Operations?             <ul style="list-style-type: none"> <li>○ If Offensive, is the capability delivered by the installation Fire Department, installation Fire Department with mutual aid from the surrounding community, or solely from the surrounding community?</li> <li>○ For Offensive Operations, are the following requirements met:                 <ul style="list-style-type: none"> <li>▪ At least seven (7) personnel on scene trained and certified to the HAZMAT Technician level?</li> <li>▪ At least one (1) person on scene trained and certified to the HAZMAT Incident Commander level?</li> <li>▪ At least five (5) personnel on scene trained and certified to at least the HAZMAT Operations level?</li> <li>▪ At least two (2) personnel on scene trained and certified to at least the EMT BLS level and shall have on-scene medical transport capability?</li> <li>▪ Available for immediate response 24/7?</li> </ul> </li> <li>○ For Defensive Operations, is there a minimum of a single engine company consisting of four (4) personnel on scene?                 <ul style="list-style-type: none"> <li>▪ Are all personnel trained and certified to at least the HAZMAT Operations level?</li> </ul> </li> </ul> </li> <li>• Can the installation F&amp;ES meet travel and response times IAW DODI 6055.06, <i>DOD Fire and Emergency Services (F&amp;ES) Program</i>?             <ul style="list-style-type: none"> <li>○ If not, what actions have been taken to mitigate the deficiency?</li> <li>○ Has the deficiency been reported up the chain-of-command?</li> </ul> </li> <li>• Are F&amp;ES telecommunicators certified as Telecommunicator I or II per DOD 6055.06-M and NFPA 1061?             <ul style="list-style-type: none"> <li>○ Are they capable of speaking bilingually when required at OCONUS locations and some CONUS locations?</li> </ul> </li> <li>• Does the Fire Chief or designated representative attend the ATWG and/or IEMWG?</li> <li>• Is a F&amp;ES representative involved in developing IEM/AT exercise scenarios?</li> <li>• Are installation grid maps posted, current, and accurate?</li> </ul>	<p>DOD Std 20 DODI 2000.16</p> <p>DODI 2000.18, Guideline 3</p> <p>DODI 6055.dd</p>
------------------	---	---

**FOR OFFICIAL USE ONLY**

EM-PLN-17	<p><b>F&amp;ES HAZMAT/CBRNE INCIDENT RESPONSE CAPABILITY</b></p> <p><b>Personal Protective Equipment (PPE):</b></p> <ul style="list-style-type: none"> <li>• Are F&amp;ES personnel trained and certified under the FF Certification System to the appropriate HAZMAT level to meet the established department operational capability?</li> <li>• What HAZMAT level are F&amp;ES personnel trained to (Awareness, Operations, Technician, Incident Command (IC))?             <ul style="list-style-type: none"> <li>○ Are certifications current and documented?</li> </ul> </li> <li>• Do F&amp;ES personnel possess PPE for response to CBRNE/HAZMAT incidents based on the established operational capability? (i.e. Level A, B, C protective clothing with positive pressure; full facepiece self-contained breathing apparatus (SCBA); positive pressure supplied air respirator with escape; full-face or half-mask air purifying respirators.)</li> <li>• Are respirators CBRN NIOSH approved?</li> <li>• Are personnel who wear PPE trained and certified IAW OSHA 29 Code of Federal Regulations (CFR) 1910.120, Hazardous Waste Operations and Emergency Response and 1910.134, Respiratory Protection?</li> <li>• Are personnel who wear NIOSH-certified respirators enrolled in a respiratory protection program?</li> <li>• Is a current inventory maintained on of all PPE?</li> <li>• Is PPE serviceable and ready for immediate use?</li> <li>• Are procedures established for tracking PPE shelf-life?</li> </ul> <p><b>Detection and Decontamination Equipment:</b></p> <ul style="list-style-type: none"> <li>• What type of detection / monitoring equipment does the F&amp;ES possess for CBRNE / HAZMAT incidents?</li> <li>• Is there a current inventory of all detection equipment?</li> <li>• How is detection equipment repaired or serviced?</li> <li>• Does the F&amp;ES possess a plume-modeling capability ie., Hazard Prediction and Assessment Capability (HPAC), Consequence Assessment Tool Set Joint Assessment of Catastrophic Events (CATS / JACE or CJ), Computer-Aided Management of Emergency Operations (CAMEO), Joint Effects Model (JEM), Reach-back capability (DTRA), etc.</li> <li>• Are SOPs developed for plume modeling?             <ul style="list-style-type: none"> <li>○ Do procedures specifically describe who, what, when, where, and how plume modeling is conducted?</li> <li>○ How does the IC receive accurate and current weather data?</li> </ul> </li> <li>• Is F&amp;ES tasked to perform mass decontamination of victims following CBRNE / HAZMAT incidents?</li> <li>• What types of decontamination equipment does the F&amp;ES possess?</li> <li>• Do F&amp;ES SOPs describe who, what, when, where, and how mass decontamination is conducted?             <ul style="list-style-type: none"> <li>○ Is guidance included in the IEM Plan?</li> </ul> </li> <li>• Are MOU / MOA / MAAs established with the local community and/or host-nation if no decontamination capability exists?</li> <li>• Are MOU / MOA / MAAs current and been exercised?</li> <li>• Is there a current inventory of all decon equipment?</li> <li>• Are procedures developed for tracking equipment shelf-life?</li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p>DODI 2000.18, Guidelines 3, 6, 7, &amp; 9</p> <p><b>DODI 6055.06</b></p> <p>Strategic Goal 2G</p>
-----------	--	---

## FOR OFFICIAL USE ONLY

EM-PLN-18	<p><b>SECURITY FORCES (SF) INCIDENT RESPONSE</b></p> <ul style="list-style-type: none"> <li>• Has SFs developed incident response SOPs based on specific taskings in the IEM and/or AT Plan?</li> <li>• Do SOPs address: <ul style="list-style-type: none"> <li>○ Establishing command and control consistent with the NIMS and ICS?</li> <li>○ Securing a perimeter around CBRNE/HAZMAT incident?</li> <li>○ Initiating evacuation or shelter-in-place actions?</li> <li>○ Establishing entry / exit traffic control points?</li> <li>○ Establishing safe routes for emergency response vehicles?</li> <li>○ Considerations for a secondary device?</li> <li>○ Searches for secondary devices conducted in conjunction with EOD team members?</li> <li>○ Scene, evidence preservation, and chain of custody?</li> </ul> </li> <li>• Are procedures established to verify/permit entry of local community emergency response vehicles onto the installation during higher FPCONs?</li> <li>• Do SFs receive incident response training i.e., HAZMAT Awareness, IED recognition, etc.?</li> <li>• Are SF dispatch operators trained and certified?</li> <li>• Are installation grid maps posted, current, and accurate?</li> </ul>	<p>DOD Std 20 DODI 2000.16</p> <p>DODI 2000.18, Guideline 3</p> <p style="color: red;">DODI 6055.dd</p>
EM-PLN-19	<p><b>SF INCIDENT RESPONSE CAPABILITY</b></p> <p><b>Personal Protective Equipment (PPE):</b></p> <ul style="list-style-type: none"> <li>• What level of operational capability has SFs established i.e., HAZMAT Awareness, Level C PPE, conduct cordon in the cold / warm zone, etc.? <ul style="list-style-type: none"> <li>○ Are personnel trained and certified to this level?</li> <li>○ Are personnel appropriately equipped?</li> </ul> </li> <li>• Do SF personnel possess PPE for response to CBRN incidents, i.e. protective mask, rubber gloves, tyvek suit, etc.? <ul style="list-style-type: none"> <li>○ Are masks NIOSH-approved?</li> <li>○ Are suits and masks properly fitted?</li> <li>○ Are personnel trained and certified IAW OSHA 29 CFR 1910.120 and 1910.134?</li> <li>○ For contracted civilian SFs / guards: the statement of work has to state whether CBRNE equipment, training, and certification or awareness course can be implemented.</li> </ul> </li> <li>• Are contract Security Guards provided PPE? If not, what work-around procedures are developed to ensure their safety and maintain security of their post?</li> <li>• Are personnel who wear NIOSH-certified respirators enrolled in a respiratory protection program?</li> <li>• Is there a current inventory of all PPE?</li> <li>• Is equipment serviceable and ready for immediate use?</li> <li>• Are procedures developed for tracking PPE and equipment shelf-life?</li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p>DODI 2000.18, Guidelines 3, 6, 7, &amp; 9</p> <p>Strategic Goal 2G</p>

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

<p>EM-PLN-20</p>	<p><b>MEDICAL RESPONSE</b></p> <ul style="list-style-type: none"> <li>• Does the installation possess a mass casualty (MASCAL) response capability?</li> <li>• Where does emergency medical response come from: installation fire department, clinic/hospital, local community, or host-nation?</li> <li>• What level are emergency medical technicians (EMT) trained: combat life saver (CLS), EMT-Basic (EMT-B), EMT-Intermediate (EMT-I), or EMT Paramedic (EMT-P)?</li> <li>• Are ambulances available from the installation and local community to support a MASCAL incident within the first hour (golden hour)?             <ul style="list-style-type: none"> <li>○ What level are ambulances equipped: basic life support (BLS) or advanced life support (ALS)?</li> </ul> </li> <li>• Is helicopter medical evacuation available?             <ul style="list-style-type: none"> <li>○ Where does it come from and what is the response time?</li> </ul> </li> <li>• What type of communications (radios, cell phones, pagers) do medical first responders possess?             <ul style="list-style-type: none"> <li>○ Is this equipment adequate?</li> <li>○ Is communications equipment compatible with host nation radios or are mitigating measures implemented?</li> </ul> </li> <li>• Are MASCAL response kits available and ready?             <ul style="list-style-type: none"> <li>○ How many casualties will each kit support?</li> </ul> </li> <li>• Are installation grid maps posted, current, and accurate?</li> </ul>	<p>DOD Std 20 DODI 2000.16</p> <p>DODI 2000.18, Guideline 3 DODI 6055.dd</p>
<p>EM-PLN-21</p>	<p><b>MEDICAL INCIDENT RESPONSE CAPABILITY</b></p> <p><b>Personal Protective Equipment (PPE):</b></p> <ul style="list-style-type: none"> <li>• What level of operational capability has been established for medical responders i.e., HAZMAT Awareness/Operations, Level C PPE, patient decontamination?             <ul style="list-style-type: none"> <li>○ Are medical personnel trained and certified to this level?</li> <li>○ Are they appropriately equipped?</li> </ul> </li> <li>• Are personnel who wear PPE trained and certified IAW OSHA 29 CFR 1910.120 and 1910.134?</li> <li>• Are personnel who wear NIOSH-certified respirators enrolled in a respiratory protection program?</li> <li>• Do medical personnel possess appropriate PPE to transport decontaminated patients if tasked, i.e., protective mask, tyvek suit, gloves, etc.?</li> <li>• Do medical personnel possess appropriate PPE to conduct patient decontamination operations, if tasked?</li> <li>• Is a current inventory of all PPE available and accurate?</li> <li>• Is equipment serviceable and ready for immediate use?</li> <li>• Are procedures developed for tracking equipment shelf-life?</li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p>DODI 2000.18, Guidelines 3, 6, 7, &amp; 9</p> <p>Strategic Goal 2G</p>

## FOR OFFICIAL USE ONLY

	<p><b>Detection and Decontamination Equipment:</b></p> <ul style="list-style-type: none"><li>• Does the installation hospital / clinic possess a decontamination capability?</li><li>• Does the medical decontamination team possess detection / monitoring equipment for CBR incidents?</li><li>• How is detection equipment repaired or serviced?</li><li>• Does the decontamination capability meet or exceed the standards set forth by the National Fire Protection Agency (NFPA) 472, Joint Commission on Accreditation of Healthcare Organizations (JCAHO) E.C.1.4., or Service directed requirement?</li><li>• Are SOPs developed that clearly describe who, what, when, where, and how in-place patient decontamination is conducted?<ul style="list-style-type: none"><li>○ Are these procedures included the Medical Response Plan?</li></ul></li><li>• Are decontamination team members trained and is training documented?</li><li>• Is there an inventory of all decontamination equipment?<ul style="list-style-type: none"><li>○ Is equipment serviceable and ready for immediate use?</li><li>○ Is shelf-life equipment items tracked?</li></ul></li><li>• Has a decontamination site been pre-identified with run-off containment considered?</li><li>• What are the methods adopted for victim decontamination?</li><li>• Are MOU / MOAs established with local / host-nation medical facilities who will accept contaminated patients?</li><li>• Are procedures established for transporting decontaminated casualties from the incident site to the nearest medical facility?</li><li>• Do ambulances have patient covers and blankets for ambulatory and litter patients after the decontamination process?</li><li>• For installations with contract ambulance services, are CBRNE planning considerations required of the EMS included in the contract statement of work?</li><li>• Are antidote injectors (i.e. CANA and NAAKs) or pharmaceuticals and vaccines available?</li></ul>	
--	---	--

**FOR OFFICIAL USE ONLY**

<p>EM-PLN-22</p>	<p><b>EXPLOSIVE ORDNANCE DISPOSAL (EOD) INCIDENT RESPONSE</b></p> <ul style="list-style-type: none"> <li>• Does the installation have an EOD team assigned? If not, where does EOD support come from? <ul style="list-style-type: none"> <li>○ Is support available 24/7?</li> <li>○ Has a MOU been developed for EOD support?</li> </ul> </li> <li>• Are EOD notification procedures developed and who makes initial contact?</li> <li>• What is the EOD response time?</li> <li>• Has the supporting EOD team reviewed the installation bomb threat/search plan?</li> <li>• Has EOD conducted a site survey to become familiar with the installation?</li> <li>• Are installation grid maps posted, current, and accurate?</li> <li>• Does EOD provide IED recognition, bomb threat / search classes?</li> <li>• Does a EOD representative attend the ATWG?</li> <li>• Is EOD involved in developing scenarios for AT and IEM exercises?</li> <li>• What type of communications does EOD possess? <ul style="list-style-type: none"> <li>○ How is communication interoperability conducted between EOD and other installation responders and the EOC?</li> <li>○ Is communication equipment compatible with host-nation equipment or are mitigating measures implemented?</li> </ul> </li> <li>• Does the installation have communication connectivity with responding EOD teams? (Most EOD teams have cellular phones)</li> <li>• Does EOD have access to SIPRNet?</li> </ul>	<p>DOD Std 20 DODI 2000.16</p> <p>DODI 2000.18, Guideline 3</p> <p><b>DODI 6055.dd</b></p>
<p>EM-PLN-23</p>	<p><b>EOD RESPONSE CAPABILITY</b></p> <p><b>Personal Protective Equipment (PPE):</b></p> <ul style="list-style-type: none"> <li>• What level of operational capability has EOD established (HAZMAT Operations, Technician Level)? <ul style="list-style-type: none"> <li>○ Are EOD technicians trained and certified to this level?</li> <li>○ Are they appropriately equipped?</li> </ul> </li> <li>• Do EOD personnel possess adequate PPE for CBRNE response?</li> <li>• Are self-contained breathing apparatus (SCBA) respirators CBRNE approved by NIOSH?</li> <li>• Is there an inventory of all PPE?</li> <li>• Is equipment serviceable and ready for immediate use?</li> <li>• Are shelf-life equipment items tracked?</li> <li>• How is equipment maintained?</li> <li>• Are personnel who wear PPE trained and certified IAW OSHA 29 CFR 1910.120 and 1910.134?</li> <li>• Are personnel who wear NIOSH-certified respirators enrolled in a respiratory protection program?</li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p>DODI 2000.18, Guidelines 3, 6, 7, &amp; 9</p> <p>Strategic Goal 2G</p>

**FOR OFFICIAL USE ONLY**

	<p><b>Detection Equipment:</b></p> <ul style="list-style-type: none"> <li>• What type of detection / monitoring equipment does EOD possess for CBR incidents? (If none, is there coordination with F&amp;ES or HAZMAT team to use or augement needed equipment?)</li> <li>• Is there a current inventory of all detection equipment?</li> <li>• Is detection equipment repaired or serviced?</li> <li>• Have MOU/MOA/MAAs been developed with the local community or host nation to ensure proper detection / monitoring equipment is available?</li> </ul> <p><b>Safe Havens:</b></p> <ul style="list-style-type: none"> <li>• Are Safe Havens designed IAW UFC 4-023-10, Security Engineering Design for Safe Havens?</li> </ul>	
EM-PLN-24	<p><b>PUBLIC AFFAIRS OFFICE (PAO)</b></p> <ul style="list-style-type: none"> <li>• Are PAO roles and responsibilities in supporting the AT/IEM Program included in the IEM Plan?</li> <li>• Are procedures developed for releasing information on emergency incidents?</li> <li>• Do procedures identify personnel to respond to the scene, escort media, and run the media center?</li> <li>• Do PAO personnel have adequate communications? (Radio / cell phone / pager)</li> <li>• Has a facility been identified to serve as the Joint Information Center (JIC) to brief media in the event of an incident? <ul style="list-style-type: none"> <li>○ Has an alternate JIC been identified?</li> <li>○ Does the JIC have back-up power if required?</li> </ul> </li> <li>• Is the PAO part of the ATWG/IEMWG?</li> <li>• Is the PAO involved in installation AT/IEM exercises?</li> <li>• Have AT/IEM articles been published in the paper and with what frequency?</li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p>DODI 2000.18, Guideline 3</p> <p>DOD O- 2000.12-H, Chapter 19</p> <p>Strategic Goal 2D</p>
EM-PLN-25	<p><b>MAIL FACILITY RESPONSE MEASURES</b></p> <ul style="list-style-type: none"> <li>• Has the mail facility developed written SOPs that address procedures personnel must take upon encountering a suspicious envelope or package?</li> <li>• Does the SOP address: <ul style="list-style-type: none"> <li>○ Isolating the envelope / package?</li> <li>○ Securing the area?</li> <li>○ Isolate / shutoff HVAC or air handling systems / equipment?</li> <li>○ Evacuating the facility / quarantine potentially exposed personnel?</li> <li>○ Notifying emergency responders?</li> <li>○ Conducting personnel decontamination if warranted i.e., washing hands with warm soapy water?</li> <li>○ Donning personnel protective equipment (NIOSH-approved respiratory protection mask and nitrile / vinyl or other OSHA approved gloves)?</li> </ul> </li> <li>• Are personnel trained in the use of issued PPE?</li> <li>• Do personnel conduct exercises for responding to the discovery of a suspicious envelope or package?</li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p>US Postal Service Publication 166</p> <p>DOD O- 2000.12-H, App 19</p> <p>COCOM AT OPORD</p>

**FOR OFFICIAL USE ONLY**

<p>EM-PLN-26</p>	<p><b>MEASURES FOR OFF-INSTALLATION FACILITIES, HOUSING, AND ACTIVITIES</b></p> <p>Installation commanders shall develop in their overall AT programs' specific AT measures for off-installation facilities, housing, transportation services, daycare centers, and other activities used by or involving a mass-gathering of DOD personnel and their dependent family members. These risk mitigation measures shall include, but are not limited to, emergency notification and recall procedures; guidance for selection of off-installation housing, temporary billeting, and other facility use (including compliance with Unified Facilities Criteria (UFC) 04-010-01 for leased, newly constructed, and expeditionary buildings); physical security measures; CBRNE defensive measures; and shelter-in-place, relocation, and evacuation procedures.</p> <ul style="list-style-type: none"> <li>• Have emergency notification procedures been developed for alerting off-installation facilities, housing areas, primary gathering building (50 or more DOD personnel), etc. of an all-hazards incident?</li> <li>• Do procedures identify who, what, when, where, and how personnel conduct evacuations or shelter-in-place procedures?</li> <li>• Are these procedures addressed in the IEM or AT Plan?</li> <li>• Are personnel trained to conduct these procedures and have they been exercised?</li> </ul>	<p>DOD Std 15 DODI 2000.16</p> <p>Strategic Goal 2G</p>
<p>EM-PLN-27</p>	<p><b>PERSONNEL CATEGORIZATION</b></p> <ul style="list-style-type: none"> <li>• Has the Installation Commander categorized all assigned personnel and provided PPE in the following priority? (DOD installations shall categorize their personnel for the purpose of accurately identifying their protected population and effectively managing their personnel resources.) <ul style="list-style-type: none"> <li>○ <u>Emergency Responders and First Responders</u>. Personnel who work closest to known or suspected hazards or threats (e.g., first responders and first receivers, law enforcement, F&amp;ES.)</li> <li>○ <u>Critical Personnel</u>. Personnel deemed essential to the performance of critical military missions (whether military, civilian, contractor, host-nation personnel, or third country nationals.)</li> <li>○ <u>Essential Personnel</u>. Personnel deemed essential to the performance of essential military operations (whether military, civilian, contractor, host nation, or third country nationals.)</li> <li>○ <u>Other Personnel</u>. All persons not covered in the previous categories. Where appropriate, installation commanders shall ensure the appointment of personnel in writing and ensure that each has received the required equipment, training, and certifications.</li> </ul> </li> </ul>	<p>DOD Std 21 DODI 2000.16</p> <p>DODI 6055.dd</p>

## FOR OFFICIAL USE ONLY

EM-PLN-28	<p><b>RECOVERY</b></p> <p>Recovery activities often extend long after the incident itself. Short-term recovery actions seek to restore lifeline systems (e.g. power, communication, water and sewage, and transportation) and ensure that the societal needs of individuals and the community are met (e.g., maintain the rule of law, provide crisis counseling, demonstrate that people do care and that help is coming.) Once some level of stability is achieved, the installation can begin restoring institutions to suitable economic growth and confidence, rebuilding destroyed property, and reconstituting government operations and services. During the recovery phase, the installation shall:</p> <p><u>Establish a Recovery Working Group (RWG).</u> A RWG shall be established early in the recovery phase of every emergency where, in the judgment of the Commander, recovery operations require coordination. The RWG is a task-organized working group focused on the evaluation, prioritization, and coordination of recovery requirements.</p> <ul style="list-style-type: none"><li>• Has the installation pre-identified members for a RWG?</li></ul> <p><u>Conduct Damage Assessments.</u> The Public Works / Civil Engineering asset may conduct physical damage assessments if such a capability exists within the installation.</p> <ul style="list-style-type: none"><li>• Has the installation Public Works / Civil Engineering developed an organic damage assessment capability and limited debris clearance capability? (These capabilities should support short-term (less than two weeks in duration) recovery efforts and initial damage assessments, resource projections, and recovery planning requirements.)</li></ul> <p><u>Identify Recovery Priorities.</u> Installation commanders shall establish recovery priorities consistent with the installation mission. Consideration shall be given to Operational Mission priorities and re-establishment of the normal operating environment.</p> <p><u>Conduct Recovery Planning.</u> The RWG (formed pre- or post-incident), with the technical direction of the Installation Emergency Manager and the Installation Public Works / Civil Engineering representative, shall conduct recovery planning at the installation level. While the Installation EM Plan facilitates response and short-term recovery, the recovery plan should provide detailed, incident-specific processes and procedures, to include immediate restoration of transportation and communication capabilities, search and rescue operations, utility reconstructions, community reconstructions, site remediation's, medical care or mitigations, and other activities necessary for successful long-term recovery.</p> <p><u>Establish Fatality Management and Mortuary Affairs</u></p> <ul style="list-style-type: none"><li>• Has the Installation Emergency Manager coordinated with appropriate functional areas to establish procedures for ensuring effective fatality management?</li><li>• Does fatality management planning include:<ul style="list-style-type: none"><li>○ Scene documentation; collection; and recovery of human remains, personal effects, and items of evidence?</li></ul></li></ul>	DODI 6055.dd
-----------	--	-----------------

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

	<ul style="list-style-type: none"><li>○ Decontamination of remains and personal effects (if required)?</li><li>○ Transportation, storage, documentation, and recovery of forensic and physical evidence?</li><li>○ Determination of the nature and extent of injury?</li><li>○ Identification of fatalities, certification of the cause and manner of death, processing, and returning human remains and personal effects to legally authorized person(s)?</li><li>○ Interaction with and provision of required legal, customary, compassionate, and culturally competent services to the family of the deceased?</li></ul>	
--	---	--

**FOR OFFICIAL USE ONLY**

<b>3. AT TRAINING AND EXERCISES</b>		
<p>EM-TE-01</p>	<p>Installation commanders shall ensure that AT training and exercises are integrated with overall physical security and afforded the same emphasis as combat task training and executed with the intent to identify shortfalls affecting the protection of personnel and assets against terrorist attack and subsequent terrorism consequence management efforts.</p> <p>Ensure that annual AT exercises encompass all aspects of AT and physical security plans. Additionally, the current baseline FPCON through FPCON CHARLIE measures shall be exercised at installations and separate facilities. Commanders will implement AT measures through FPCON DELTA at parts of the installation. The ATO shall develop an annual training and exercise program to provide the necessary individual and collective training to prepare for the annual exercise.</p> <p>Conduct comprehensive field and staff training, including deploying units (battalion, ship, squadron, equivalent-sized units, and above) to exercise AT Plans at least annually. Ensure that annual AT exercises encompass all aspects of AT and physical security plans. Additionally, the current baseline FPCON through FPCON CHARLIE measures shall be exercised at installations and separate facilities.</p> <ul style="list-style-type: none"> <li>• Has the installation developed an AT Training and Exercise Program and included guidance in the AT Plan or referenced its location?</li> <li>• Does the installation training program provide for the necessary initial and periodic refresher training consistent with the threat and appropriate to the different emergency responsibilities?</li> <li>• Is AT training incorporated into unit-level training plans and pre-deployment exercises?</li> <li>• Does the annual AT exercise encompass all aspects of AT Plan and associated plans?</li> <li>• Are exercise scenarios based on the installation local Hazard / Threat Assessment?</li> <li>• Is the installation or COCOM design basis threat (DBT) exercised?</li> <li>• Are MASCAL exercises conducted?</li> <li>• Is the current baseline FPCON through FPCON CHARLIE exercised by the installation and separate facilities?</li> <li>• Is FPCON DELTA implemented at parts of the installation?</li> <li>• Are evacuation and shelter-in-place (SIP) procedures exercised?</li> <li>• Are after action reports and lessons learned developed?</li> <li>• Is AT exercise documentation maintained for at least two years?</li> <li>• If OCONUS, does the host nation participate in training exercises and initial planning?</li> </ul>	<p>DOD Std 23 DODI 2000.16</p> <p>DODI 2000.18, Guideline 5</p> <p>Strategic Goal 3F</p>

**FOR OFFICIAL USE ONLY**

EM-TE-02	<p><b>INSTALLATION EXERCISE EVALUATION TEAM (IEET)</b></p> <ul style="list-style-type: none"> <li>• Has the Installation Commander established an IEET? (IEET shall evaluate the capability of the installation to respond to any incident using an all-hazards approach to EM.)</li> <li>• Does the composition of the IEET include individuals with experience in EM who are familiar with the Homeland Security Exercise and Evaluation Program (HSEEP), Volume III, Exercise Evaluation and Improvement Planning? <ul style="list-style-type: none"> <li>○ <a href="https://hseep.dhs.gov/support/VolumeIII.pdf">https://hseep.dhs.gov/support/VolumeIII.pdf</a></li> </ul> </li> </ul>	DODI 6055.dd
EM-TE-03	<p><b>IEM TRAINING</b></p> <ul style="list-style-type: none"> <li>• Has an education and training program been established to create awareness across the installation and to enhance the skills of individual’s assigned EM functions or responsibilities?</li> <li>• At a minimum, does IEM education and training encompass the following: <ul style="list-style-type: none"> <li>○ Ensure appropriate training of designated Installation Emergency Managers tasked with overseeing and implementing IEM Programs and plans? (Shall be fully trained in appropriate ICS and EM concepts and policies in order to fulfill the responsibilities of this role.)</li> <li>○ Emergency First Responders and Receivers trained in appropriate ICS, Emergency Medical Services (EMS), HAZMAT, and task-specific training? (All EMS and HAZMAT training should be IAW part 1910.120 of title 29, Code of Federal Regulations (Reference (s)); NFPA Consensus Standards 472 and 473 (References (t) and (u)); and Occupational Safety and Health Administration’s (OSHA) “OSHA Best Practices for Hospital-Based First Receivers of Victims from Mass Casualty Incidents Involving the Release of Hazardous Substances.”</li> <li>○ Community awareness? IEM community awareness and emergency preparedness information shall be made available to all assigned personnel</li> <li>○ New equipment training? As new IEM equipment is deployed, personnel assigned EM responsibilities requiring use of the new equipment shall be trained IAW Service policy and procedures regarding new equipment.</li> </ul> </li> <li>• Has the Installation Commander’s staff, ATO, Installation Emergency Manager, EOC staff, and emergency responders completed the Federal Emergency Management Agency Independent Study Courses? <ul style="list-style-type: none"> <li>○ IS-100.a Introduction to Incident Command System (ICS)</li> <li>○ IS-200.a ICS For Single Resources and Initial Action Incidents</li> <li>○ IS-700 National Incident Management System (NIMS), An Introduction</li> <li>○ IS-800.B National Response Framework (NRF), An Introduction</li> </ul> </li> </ul>	DODI 6055.dd

## FOR OFFICIAL USE ONLY

EM-TE-04	<b>IEM EXERCISES</b> <ul style="list-style-type: none"><li>• Do exercises assess and validate proficiency levels, clarify and familiarize personnel with roles and responsibilities, improve interagency coordination and communication, highlight capability gaps, and identify opportunities for improvement?</li><li>• Do exercises:<ul style="list-style-type: none"><li>○ Include multi-disciplinary, multi-jurisdictional incidents?</li><li>○ Include participation of appropriate leaders and decision makers representing each of the emergency response functions on the installation, and, whenever possible, appropriate local, state, tribal, other Military Service(s), host-nation, private-sector, and nongovernmental organization (NGO) partners?</li></ul></li><li>• Are the following components of the IEM Plan and/or EM response capabilities assessed:<ul style="list-style-type: none"><li>○ Activation of local support agreements (e.g., MAAs, MOUs, MOAs, SOFAs)?</li><li>○ Execution of notification protocols, both internal (installation personnel only), and external (with local, state, tribal, other Military Service(s), and host-nation partners)?</li><li>○ Mass warning and notification?</li><li>○ Command, control, and communication?</li><li>○ First responders and receivers?</li><li>○ Emergency operators and specialists?</li><li>○ Medical response?</li></ul></li><li>• Are exercises conducted annually, at a minimum? (EM exercises may be conducted in coordination with, or as a part of other, tabletop, full scale, or functional exercises (e.g., AT and force protection exercises.))</li><li>• Do exercises include a thorough and objective exercise evaluation process? During the exercise and upon its conclusion, the evaluation team, functional participants, and leadership shall evaluate performance against relevant capability, identify deficits, and institute after-action reporting. After-action reporting and improvement planning shall develop specific recommendations for changes in practice, timelines for implementation, and assignments for completion, to include incorporation of lessons learned into the annual IEM Plan update and review process.</li><li>• Do exercises contain a mechanism for incorporating corrective actions through the development of an after-action report?</li><li>• At the end of each exercise, do installations conduct formal reviews among exercise participants and observers of EM actions performed successfully, outcomes achieved, lessons learned, and areas for improvement derived from the exercise?</li><li>• Upon completion of the after-action reports, is a corrective action plan developed and implemented and the results incorporated into the annual IEM Plan review and update process?</li><li>• Is there a mechanism for incorporating corrective actions through the development of an after-action report?</li></ul>	DODI 6055.dd
----------	---	-----------------

**FOR OFFICIAL USE ONLY**

<b>4. AT RESOURCE APPLICATION</b>		
EM-RA-01	<p>Installation commanders shall assess the risk against the standard and apply mitigation measures. Where the resulting risk is still deemed too great, elevate the vulnerability using the PPBE process and implement the DOD or Service HQs-approved methodology and guidance for documenting and prioritizing resource requests.</p> <ul style="list-style-type: none"> <li>• Has the Installation Emergency Manager developed a process for requesting funds to mitigate equipment shortfalls of the IEM Program and CBRNE Emergency Response Program? [Coordinate with Security Operations.]</li> <li>• Are Emergency Management vulnerabilities added to and updated in the Core Vulnerability Assessment Management Program (CVAMP)?</li> </ul>	<p>DOD Std 30 DODI 2000.16</p> <p>DODI 2000.18, Guideline 1</p> <p>Strategic Goal 4A</p>
<b>5. AT PROGRAM REVIEW</b>		
EM-PR-01	<p>Installation commanders shall conduct comprehensive Program Reviews to evaluate the effectiveness and adequacy of AT Program implementation.</p> <ul style="list-style-type: none"> <li>• Is the Commander conducting an annual review of the IEM and CBRNE Emergency Response Program to facilitate program enhancement and to ensure compliance with DODI 2000.16, DODI 2000.18, and DODI 6055.dd?</li> <li>• Does the Program Review evaluate the installation’s ability to respond to the hazards identified in the installation Hazard Assessment?</li> <li>• Is the Defense Continuity Program part of the Program Review?</li> </ul>	<p>DOD Std 31 DODI 2000.16</p> <p>DODI 2000.18 Guideline 4</p> <p>Strategic Goal 5C</p>