Joint Staff / Defense Threat Reduction Agency
Vulnerability Assessment Benchmarks
1 January 2008

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 Benchmarks

1. AT RISK MANAGEMENT		
TO-RM-01	**Risk Management.** AT Risk Management process shall be performed IAW HHQ guidance and the 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 the prioritization and allocation of resources. • Does AT Risk Management include the following essential elements/components? o Threat Assessment o Criticality Assessment o Vulnerability Assessment o Risk Assessment • Does the AT Risk Management process outline o Capabilities to deter terrorist incidents? o Employ countermeasures? • Are mitigation options identified? • Is a person or entity assigned for supervising the integration of risk management across the spectrum?	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
TO-RM-02	**Threat Assessment.** 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. • Is the TA current? • Is the TA updated annually or more frequently as the terrorist threat environment dictates? • Does the TA use the DoD Terrorism Threat Analysis Methodology? (Operational Capability, Intentions, Activity, Operating Environment) o Is the threat level identified by DIA used by the installation? [Installation commanders cannot set their own Threat Level] (DoD Std 2) o If different than the DIA threat level, did the COCOM set the threat level?, (if applicable) Does the TA use the Defense Threat Assessment (DTA) Format? • Does the TA identify the full range of feasible (known or estimated terrorist capabilities (weapons, tactics, techniques, and methods of attack)? • 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 not a requirement] • 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.	DoD Std 4 JP 3-07.2, Ch III, VI, & AP B DoD 2000.12 E4.1.16 DoD O-2000.12-H, Chapter 5 Strategic Goal 1E UFC 4-020-01, Ch. 3

	○ Are local toxic industrial chemicals/toxic industrial materials (TIC/TIM) identified? [Include those that transit the installation or in close proximity] • Are the terrorist COA's integrated into the TA? (Not a requirement, possible best practice if developed). • Is there a process to integrate and fuse all source information? [strategic, operational, and tactical (local) intelligence products] ○ Strategic - DIA, CIA, DOJ, DOS, NSA, DHS ○ Operational – Services (Army Counterintelligence Center (ACIC), Naval Criminal Investigative Service (NCIS), Air Force Office of Special Investigations (AFOSI), COCOM J-2s and Intelligence Centers ○ Local, State, Federal (FBI) and host-nation law enforcement agencies? ○ Appropriate local State, Federal, and host-nation Intelligence Community (IC) activities? ○ Applicable U.S. country team; port authority officials and husbanding contractors? • Is the assessment tailored to the local environment? • Is the TA integrated into the AT Program? ○ Integrated into risk management? ○ Justification for implementation of RAMs? [Coordinate with Security Operations] ○ Physical Security changes? [Coordinate with Security Operations] ○ Program and budget requests? ○ Used when conducting VAs, especially the Design Basis Threat? ○ Is the TA used as the basis to provide justification for changes to the FPCONs? [review through the TWG and ATWG (Security Operations)] • Are specific threat assessments 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?	
TO-RM-03	**Criticality Assessment.** A criticality assessment (CA) shall be established and updated annually IAW HHQ guidance. • Is the CA current? • Does the CA comply with HHQ guidance? • Has some mission analysis been conducted to identify mission critical assets using: ○ DoD Directives - Universal Joint Task List (UJTLs) ○ COCOM Directives – OPLANS, Joint Mission Essential Task List (JMETL) ○ Service Directives – Mission Essential Task List (METL) ○ Commander's priorities • Does the CA identify, classify, and prioritize mission-essential assets, resources and personnel critical to mission success? ○ Are tenant's critical assets included in the assessment? ○ 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]	DoD Std 5 JP 3-07.2, AP A - 1 DOD O-2000.12-H, Chapter 6 Strategic Goal 1F

	• 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 warranting protective measures? • Does the CA identify redundancies within critical functions? • Does the CA determine time required to duplicate key assets or infrastructures efforts if temporarily or permanently lost?	
TO-RM-04	**Vulnerability Assessment.** A vulnerability assessment (VA) shall be established and conducted annually IAW HHQ guidance. • 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. • Is the VA current? [Within the last 12 months] • Does the VA include mission essential assets, resources, and personnel critical to mission success that are susceptible to a terrorist attack? • Does the VA include off-installation housing, schools, daycare centers, transportation systems, and routes used by DoD personnel and their dependent family members when the terrorist threat level is SIGNIFICANT or higher? (OCONUS) • Is the VA properly classified IAW DTRA JSIVA Security Classification Guide or COCOM supplement? • Was the current TA used when conducting VAs, to include the local DBT? • Have the following actions been completed within 90 days of a completed VA: o Vulnerabilities prioritized? o Has a plan of action been developed to mitigate or eliminate the vulnerabilities? o Has the results of the VA been reported to first general officer, flag officer or civilian equivalent director in the chain of command? • Are vulnerabilities being tracked until mitigated? o Is Core Vulnerability Assessment Management Program (CVAMP) being used to track vulnerabilities? o 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) • Has a designated person/staff/unit been identified to conduct/lead the assessments? o Is the ATWG or similar organization used to perform/validate the assessments	DoD Std 6 JP 3-07.2 AP C-1 DoD O-2000.12-H, Ch. 7 & 14 Strategic Goal 1G
TO-RM-05	**Risk Assessment.** A risk assessment (RA) shall be established and conducted annually as part of the risk management process. • Does the RA comply with HHQ requirements? o Is the Joint Antiterrorism (JAT) Guide used? o Is DoD O-2000.12-H, Chapter 8 used? o Is CVAMP used? (SG 4D) o (Any of these three programs satisfy the requirement for a risk assessment product) • Is data from the TA, CA, and VA included in the RA?	DoD Std 3 JP 3-07.2 AP D-1 DoD O-2000.12-H, Chapter 8

	• Have countermeasures been identified to reduce the risk? • Has a plan of action been developed to implement the countermeasures? • Does the RA identify the amount of risk reduction gained by countermeasure implementation? • Has the RA been translated into action items for either resourcing or procedural corrections (this can also be done using CVAMP)? • Have waivers been requested when risk is accepted (if required)? • Is there a prioritization method that assists the commander with risk acceptance? • Have compensatory measures been identified for all risks that are accepted? • Is the RA conducted annually?	Strategic Goal 1H FM 3-100.12
TO-RM-06	**Design Basis Threat (DBT).** 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 designed is based. o Has the installation identified a design basis threat (DBT)? o How was the DBT developed, i.e., analysis of the threat? ▪ HHQ Directed ▪ Unified Facilities Criteria (UFC) ▪ Locally developed. (Must meet/exceed UFC/HHQ directed DBT) ▪ Threat Matrix • Does the threat assessment support the identified DBT?	DoD Std 4 JP 3-07.2, Chapter VI-14 TM 5-853, Security Engineering UFC 4-020-01; 4-010-02
2. AT PLANNING		
TO-PLN-01	**Intelligence Support to the AT Program.** AT Intelligence shall be included in the AT Program and discussed in the intelligence annex of the AT Plan. **PLANNING AND DIRECTION (TO-PLN-01A)** • 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)? • If no organic intelligence capability exists, has the commander arranged for intelligence support from either higher headquarters or other entity? • Does the AT Plan include an AT Intelligence Annex? • Have commanders Critical Information Requirements (CCIRs) and Priority Intelligence Requirements (PIR) been developed to focus collection and analysis efforts? o Are applicable COCOM, Military Departments, Defense Agencies, and Field Activities CCIRs and PIRs incorporated? (Including terrorist capability to acquire and use WMD). o Have FBI and DHS PIR been considered? (USNORTHCOM) o Have factors which are associated with indicators and warnings of increased terrorist activity been defined? • Has counter surveillance, surveillance detection and counterintelligence been integrated into the installation's AT Program? **COLLECTION (TO-PLN-01B)**	DoD Std 2 E4.4.2.10 JP 3-07.2 AP B, E, K & Fig K-1 DoD O-2000.12-H, Chapter 5, 11 & AP 4

	• Has an AT threat information organization matrix/plan been developed based information requirements?
	  o Has the commander tasked an official to develop and maintain the AT threat information organization matrix/plan?
	  o Does the collection plan include all PIRs and CCIRs?
	  o Do tasked organizations know they are tasked and understand reporting procedures?
	  o Is liaison activity defined?
	• Are sources of strategic, operational, and tactical intelligence products identified?
	• Does the installation use the process identified by HHQ for requesting information? (includes the development and handling of information / intelligence requirements)
	
	PROCESSING AND EXPLOITATION (GENERALLY NOT USED) (TO-PLN-01C)
	
	PRODUCTION (TO-PLN-01D)
	• What intelligence products are produced locally? (may include threat assessments, threat matrix, indicators and warnings, AT articles, special assessments)
	• Is Intelligence Preparation of the Battlespace conducted to develop terrorist courses of action (COA)?
	
	DISSEMINATION (TO-PLN-01E)
	• 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., Defense Terrorism Warning Reports, and/or HHQ threat messages, OPREP-3, Blue Dart, etc.)
	  o What are the methods of transmittal?
	  o Is the TWG/ATWG involved in this process?
	  o Is a dissemination process in place to transmit threat information to appropriate personnel/commands (specifically security forces personnel)? [Verify with Security Operations]
	  o Is a process in place to notify the command when threat information is obtained?
	• 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?	

TO-PLN-02	**ATO SIPRNet Access.** 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. • Does the ATO have an Antiterrorism Enterprise Portal (ATEP) account? • Does the ATO belong to communities affiliated with his/her COCOM, and Service/Component Command? Not a requirement.	DoD Std 26 Strategic Goal 1I
TO-PLN-03	**Threat Working Group.** A Threat Working Group (TWG) should be identified as the focal point for the integration of terrorist intelligence into AT operations	DoD Std 11

	• Does the plan address composition, charter, and responsibilities including:
	  o Development and refinement of the terrorism threat assessment
	  o Coordination and dissemination of threat warnings, reports, and summaries.
	• Does the TWG integrate threat information derived from intelligence and counterintelligence sources with reports of criminal or suspicious activity derived from local law enforcement or other sources?
	  o Does the TWG identify mitigation courses of action for identified threats?
	  o Is the process for issuing threat warnings in place?
	  o Are reviews conducted when the threat changes?
	  o Do regularly scheduled meetings occur (quarterly) or as threat activity dictates or based on COCOM or AT Plan requirements?
	• Are minutes kept for each meeting and are they disseminated?
	• Is actionable information provided to the ATWG or similar activity?
		DoD O-2000.12-H, Ch. 1.2.5
		
		Strategic Goal 1B

TO-PLN-04	**Counter-Surveillance/Surveillance Detection.** The installation AT programs shall integrate counter-surveillance (CS) and surveillance detection (SD), as a matter of routine.
	• Is there a program identified for counter-surveillance and surveillance detectio
	• Are organic capabilities/tasks identified in the AT Plan?
	  o If no organic capability exists, has the commander arranged for support from either higher headquarters or other entity?
	• Are specialized skills included in the AT Plan?
	  o Has a Surveillance Detection Plan been developed?
	  o Have fixed point surveillance diagrams been developed and shared with security forces/ tenant commands/ and housing offices? (not a requirement)
	• Have procedures for reporting and investigating possible surveillance been developed?
	  o What reporting system is used? (FBI's GUARDIAN REPORTING SYSTEM for CONUS/OCONUS COCOM directed) (SG 1A)
	  o Have procedures for the neutralization and exploitation of surveillance been developed?
	  o Are individuals trained to identify/report potential terrorist surveillance?
	  o Does the installation have a neighborhood watch program? If so, are reporting procedures known throughout the military community?
		DoD Std 2 E3.2.2.4.
		
		JP 3-07.2, Chapter III
		
		DoD O-2000.12-H, AP 7

TO-PLN-05	The installation shall establish an OPSEC program that includes a Website Vulnerability Review Program to ensure that inadvertent or unauthorized disclosure of sensitive information via the world wide web is protected. • Has responsibility for the Website Vulnerability Review Program been assigned? (this could be the installation PAO) • Have procedures and guidelines been established for information provided on the DoD websites that are publicly accessible? • Are all stakeholders involved in the review process? (e.g., Webmasters, page maintainers, network administrators, SMEs, PAOs, and OPSEC personnel) • Evaluations of activity information shall follow current OPSEC procedures • How often are website reviews conducted?	DoD Std 7 E4.4.3.18. DoD O-2000.12-H Chapter 20

3. AT RESOURCE APPLICATION		
TO-RA-01	AT resource requirements shall be based on risk management products. • Has 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 VA documents and CVAMP]	DoD Std 3 JP 3-07.2 AP C-1 Strategic Goal 4F
TO-RA-02	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 out brief and written report. The Heads of DOD component 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 the Core Vulnerability Assessment Management Program (CVAMP).Risk Assessment portion of CVAMP must be filled out before funding can be submitted. • Is CVAMP used in accordance with HHQ guidance? • Is funding coded with Cbt-RIF, UFR, or local funding?	DoD Std 30 E3.30.1.3. Strategic Goal 4D
4. ILLUSTRATIVE TARGET		
	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' which are identified has having a presence in the Geographic Combatant Commanders 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 CBRN. Scenario must exploit vulnerabilities identified.	
TO-IT-01	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: • 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. • If the installation, unit, or organizational web site (.mil only) violates DoD Web Site Administration Policy, dated 7 December 1998, an observation will be written • Observations made by the Terrorist Operations Specialist that identify vulnerabilities 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.	
TO-IT-02	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. This terrorist attack cycle consists of seven distinct steps, culminating in the actual attack. These steps have been identified as: 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. 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: • Perform a general reconnaissance of the target(s) visually and supplemented with still and video photography • Video capability may include downloading to a personal computer for immediate or later transmission • Notes may be taken, strip maps drawn or maps marked • 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. 3) Final Selection: 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. 4) Planning: Specifics of the attack are determined. In this step the tactical target is clearly defined. The target and the 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. 5) Final Surveillance: 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).	

	6) Deployment: 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. 7) 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.	

Annex B
Security Operations Specialist Benchmarks

1. AT RISK MANAGEMENT		
SO-RM-01	**Personal Security Vulnerability Assessment (PSVA)**. 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. • Does the installation have a process to conduct PSVAs for HRPs? • Are PSAVs completed within 90 days of assignment to the High Risk Billets (HRB)? • Are PSVAs revalidated annually and updated if the Terrorism Threat Level changes, but no less than 3 years? • Do the PSVAs conform to the Defense Criminal Investigative Office formats?	DoD Std 6 DoD 0-2000.12-H Chapter 7 Strategic Goal 1G
SO-RM-02	**Pre-deployment Vulnerability Assessments (PSVA)**. Installation commanders shall complete pre-deployment vulnerability assessments. Procedures must comply with the HHQ's guidance such as frequency of assessments, time of VA, etc. • Does the installation's pre-deployment VA process conducted in accordance with the HHQ's guidance for air, sea, ground, and rail? • Are VAs conducted for the following: o Sea, air, and ground movements o Assembly, staging, reception, and final beddown locations • Does in-transit and/or deployment VAs include assessments of critical roads and bridges? • Do pre-deployment VAs include movement or shipping of military cargo (including Military Sealift Command voyage charters) • 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)? • Did the VA include coordination with host nation for support? • Are previous VAs used to help support and establish/develop the current VA? • Is there a process established for deploying commanders faced with emergent AT requirements to submit funding request for the procurement of necessary equipment and materials to support the required AT posture? • What process are commanders using to identify AT equipment and/or technology to their chain of command? • Are COTS and GOTS products used to meet near term AT requirements?	DoD Std 6 DoD 0-2000.12-H Chapter 7 Strategic Goal 1G
SO-RM-03	**Special Event Vulnerability Assessments**. 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. • Is there a process to ensure VAs of special events with 300 or more DoD personnel accomplished? • Is the process for special events planning included in the AT Plan? • Are specific AT Plans or Operations Orders developed for each special	DoD Std 6 DoD 0-2000.12-H Chapter 7 Strategic Goal 1G

	event? • What is the process to monitor scheduling of special events? • Does the installation have a risk assessment process for special events? (Coordinate with terrorist Options)	
SO-RM-04	**Off-Installation Asset Vulnerability Assessments**. Installation commanders shall have a process to conduct vulnerability assessments of off-installation activities and facilities in areas where the Terrorism Threat Level is **SIGNIFICANT** or higher. • Are VAs conducted for off-installation housing areas? [applicable in CONUS at DoD-owned or leased housing areas-reference current USNORTHCOM OPORD} • Does off-installation VAs, at a minimum, use the same DBT as the installation? • Are VAs conducted of DoD Dependent Schools located off the installation? [reference DoDEA AT Guidance] • Are Daycare centers located off the installation included in the VA requirements? • Are vulnerability assessments conducted on transportation systems used DoD personnel and their family members, e.g. school buses, shuttle buses, etc? • Are vulnerability assessments conducted on the routes of travel used by DoD personnel and their family members?	DoD Std 6 DoD 0-2000.12-H Chapter 7 Strategic Goal 1G
2. AT PROGRAM AND PLANNING		
*SO-PRO-01	**AT Program Elements**. The minimum required elements of a DoD AT Program shall be: • Risk Management (DoD Std 3) • Planning (including the AT Plan) (DoD Std 7) • Training and Exercises (Std 23) • Resource Application (DoD 30) • Comprehensive Program Review (DoD Std 31) • Addresses all DOD Standards • Are these elements integrated into and/or support a comprehensive AT Program?	DoD Std 1 DoD 0-2000.12-H Chapter 9 Strategic Goal 2D
*SO-PRO-02	**AT Program Coordination.** 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. • Has the commander coordinated the AT requirements with the local community? • Does coordination incorporate the information contained in the Country Memorandum of Agreement and the Status of Forces Agreement for OCONUS locations? • Does coordination include the ability to conduct FPCON measures that affect the local community? • Are tenants incorporated into the host installation's AT Program? • Are tenant security plans incorporated into the host's AT Program?	DoD Std 8 DoD 0 2000.12-H Chapter 3

*SO-PRO-03	**Antiterrorism Officer (ATO).** 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)] • Has the commander designated an ATO? • Is the ATO position a full time position? • Is an ATO designated at the battalion, ship, squadron, and separate facility level? • Is there an ATO assigned to deploying units with 300 or more personnel? • Is the CBRNE expertise available to support the ATO (assigned on staff or supporting the program)?[this is a consideration]	DoD Std 9 DoD 0-2000.12-H Chapter 9 Strategic Goal 3C

*SO-PRO-04	**Antiterrorism Executive Committee (ATEC).** 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).
	
	• Has the installation commander established an ATEC?
	• Does the ATEC meet at a minimum on a semi-annual basis?
	• Is the ATEC responsible for?
	  o Developing and refining AT Program guidance, policy, and standards
	  o Acts upon recommendations of the ATWG and TWG
	  o Determining resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities
	• Is ATEC charter captured in AT Plan?
	• Does the membership consist of as a minimum?
	  o The Installation Commander
	  o Commanders of subordinate units
	  o Commanders of tenant units
	  o Senior leaders of local first responders or host-nation (if appropriately cleared)
		DoD Std 12
		
		Strategic Goal 2B

*SO-PRO-05	**Antiterrorism Working Group.** Installation commander shall establish an Antiterrorism Working Group (ATWG).
	• Has the installation commander established an ATWG?
	• Does the ATWG meet at a minimum on a semi-annual basis or more frequently dependent upon the level of threat activity?
	• Is the ATWG responsible for?
	  o Developing and refining AT Plans
	  o Conducting vulnerability assessments
	  o Addressing emergent or emergency AT program issues
	  o Prioritizing AT resource requirements
	• Are the right functions represented in the ATWG?
	  o Does the membership consist of as a minimum?
	  ▪ The Antiterrorism Officer
	  ▪ Commander/civilian equivalent or designated representative
	  ▪ Key members of the principle staff
	  ▪ CBRNE expertise
	  ▪ Tenant unit representatives
	  ▪ Local and host-nation first responders (if appropriately cleared)
		DoD Std 10
		
		Strategic Goal 2A

	• Is the ATWG active? Keeps minutes? Accomplishes the AT functions as defined in the AT Plan and DoD O-2000.12-H?	
	AT PLAN	
*SO-PLN-01	**AT Plan.** The installation commander shall develop and maintain a comprehensive AT Plan for all DoD Elements and Personnel under their AT responsibility. • Is there an AT Plan that covers all personnel under the commander's AT responsibility? • Does the installation's AT Plan address as a minimum the following applicable areas: o The minimum essential AT Program Elements (DoD Std 1) o Specific threat risk mitigation measures to establish a local baseline defensive posture. [should incorporate the HHQ baseline] o AT Physical Security Measures (DoD Std 13) o AT Measures for Off-Installation Facilities, Housing, and Activities (DoD Std 15) o AT Measures for HRP (DoD Std 16) o AT Construction and Building Considerations (DoD Std 17) [coordinate with the Structural Engineer] o AT Measures for Logistics and Other Contracting (DoD Std 18) [coordinate with Infrastructure Engineer] o AT Measures for Critical Asset Security (DoD Std 19) [coordinate with all team members] o AT Measures for In-transit Movement o Terrorism Incident Response Measures (DoD Std 20) [coordinate with Emergency Management/CBRNE team members] o Terrorism Consequence Management Measures, including CBRNE and WMD mitigation planning (DoD Std 21) [coordinate with Emergency Management/CBRNE team members] o FPCON Implementation Measures, including Site-Specific AT Measures (DoD Std 22) o CBRN Defense Joint Enabling Concepts of Sense, Shape, Shield, and sustain per JROCM 180-3 [coordinate with Emergency Management/CBRNE team members] • 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] • Has the AT Plan been signed and exercised? Entire installation must exercise through FPCON CHARLIE [coordinate with Emergency Management Specialist] • Are AT Plans developed at the following levels beyond the installation-level: o Separate or leased facility/space o Ships o Operational deployments o Large scale Training and Exercises o Special events	DoD Std 7 DoD 0-2000.12-H Chapter 9 Strategic Goal 2D
SO-PLN-02	**AT Program Coordination**. Commanders shall initiate coordination of AT matters with the appropriate Geographic Combatant Commander. • Has AT matters been coordinated with local, State, Federal and host-nation authorities pursuant to existing law and DoD policy to support AT planning and program implementation?	DoD Std 8 DoD O-2000.12-H, Chapter 1

	• Have subordinate elements of DoD Components that are tenant units on installations or separate facilities coordinated their AT program and plan requirements with the host installation or separate facility commander or civilian equivalent director? • Is the senior DoD Component responsible for integrating and coordinating security plans into a comprehensive installation or facility-wide AT program?	
	FORCE PROTECTION CONDITION (FPCON) MEASURES	
*SO-PLN-03	**FPCON Measures.** 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). **SETTING FPCON LEVELS** • Is the policy for setting FPCON levels promulgated in the AT Plan? • Are the ATWG and TWG involved in the FPCON setting process? • Is FPCON declaration based upon the following factors, as a minimum? o Threat o Target vulnerability o Criticality of assets o Security resource availability o Operational and physiological impact o Damage control o Recovery procedures o International relations o Planned U.S. Government actions that could trigger a terrorist response **FPCON TRANSITION** • Has the installation established and published the process for transitioning between FPCON levels? • Does this process include lowering the FPCON Level and is the implementation of supplemental measures and RAM vice maintaining the higher level FPCON? o Higher-level commander's FPCON level cannot be lowered without written concurrence. **FPCON DISSEMINATION AND IMPLEMENTATION** • Has the installation established and published a process for disseminating and implementing FPCON measures? • Is there a process to determine that FPCON measures are implemented and maintained throughout the FPCON declaration? • Is there a process developed and prescribed for the notification of higher headquarters in regards to FPCON changes? • Are all mandated FPCON measures being implemented? **FPCON WAIVER PROCESS** • Have waivers been processed in writing for FPCON measures that are not being implemented?	DoD Std 22 DoD 0-2000.12-H Chapter 10 CJCSI 3121.01A DODD5210.56 Strategic Goal 2D

	• Is the waiver process in accordance with the HHQ guidance? • Are compensatory measures developed for FPCON measures that have approved waivers? [coordinate with all assessment team members] • Is a process established to annually review waiver?	
*SO-PLN-04	**Site-specific FPCON Measures**. 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. • Has the installation developed site-specific FPCON measures? • 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? • Are site-specific FPCON measures also developed for in-transit forces? • Are the site-specific FPCON measures appropriately classified? • 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) • Is 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	DoD Std 22 DoD 0-2000.12-H Chapter 10 CJCSI 3121.01A DoDD 5210.56 Strategic Goal 2D
	RANDOM ANTITERRORISM MEASURES (RAM)	
*SO-PLN-05	**Random Antiterrorism Measures (RAM).** Installation commander shall develop and implement RAM as an integral component of the overall AT Program. **RAM PROCESS** • Does the RAM program comply with HHQ guidance? • Does the RAM program change the ~~installation's~~installations AT tactics, techniques, and procedures so that they ensure a robust security posture? • Is the program unpredictable and ambiguous to instill uncertainty in terrorist planning? • Are RAMs used throughout all FPCON levels? **RAM DEVELOPMENT / IMPLEMENTATIOM** • Has the installation assessed local threat capabilities and identified effective RAM countermeasures? • 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)? • Do selected RAMs mitigate installation/facility vulnerabilities and are geared towards prevention of the DBT entering the installation/facility? • Are RAMs conducted both internally to the installation and externally in coordination with local authorities? • Are selected RAMs compatible/coordinated with ongoing approved surveillance?	DoD Std 14 DoD 0-2000.12-H, Chapter 10 Strategic Goal 2D

	• Are selected RAMs designed to detract from the terrorist attack planning capabilities (e.g., effects surveillance)? **RAM MANAGEMENT** • Is the installation ATO designated as the office responsible for the RAM program? • Does the ATO coordinate with Security Forces regarding the RAM measures that require security personnel? • Does the ATO monitor, track, and analyze RAM implementation efforts of all units? • Does the ATO conduct spot checks to determine if RAMs are being conducted? **UNIT/TENANT INVOLVEMENT** • Do all assigned and tenant units/agencies/activities support RAM program? • Are assigned units and tenants allowed to develop/implement their own RAMs? • Are tenant conducted RAMs reported to the ATO?	
	AT PHYSICAL SECURITY MEASURES	

*SO-PLN-06	**AT Physical Security Measures.** 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.
	• Does the Physical Security Program integrate and synchronize the following?
	  o Detection (human, animal, or sensors to alert security personnel of possible threats and unauthorized entry attempts at or shortly after occurrence)
	  o Assessment (electronic audio-visual means, security patrols, or fixed posts to localize and determine the size and intentions of unauthorized intrusions or activity)
	  o Delay/denial (active and passive security measures including barriers to impede intruders efforts)
	  o Communication (command and control procedures)
	  o Response (trained and properly equipped security forces)
	• Is the physical security program based on the threat and criticality assessment? (Design Basis Threat)?
	• Does the installation have a physical security plan?
	• Do measures include the development of access control procedures for ingress and egress control?
	• Is CBRNE protection included in the Physical Security Program to include the postal system?
	• Is HRP protection included in the program?
	• Is barrier planning and stand-off included in the program? [coordinate with Security Engineering]
	• Are physical security inspections / surveys conducted?
	• Are physical security deficiencies annotated and corrected?
		DoD Std 13
		
		DoD 5200.8-R
		
		DoD 0-2000.12-H Chapter 22

SECURITY FORCES		

*SO-PLN-07	**Security Force Operations**. The installation's Physical Security Program shall include the integration of security forces for detection, assessment, and response.
	
	• Is there an identified immediate response force?
	• Is the response force capable of slowing the advance of the aggressors?
	  o Facilitate the evacuation of the protected asset to safe areas?
	  o Secure the protected asset and containing the threat
	  o Prevent additional hostile resources from arriving, and prepare to apprehend the threat and relieve the protected asset.
	• Does the security forces operation planning address the following?
	  o Organization, training, and equipping of augmentation security forces
	  o Primary and alternate dispatch location
	  o Primary and alternate arming point
	  o Pre-planned response for threats (at a minimum those identified in the threat assessment)
	  o Overt attack
	  o Protection of Distinguished Visitors/HRPs
	  o Prioritized posting for FPCONs
	  o Contingency Operations
	• Does the installation have enough security forces (include augmentees) to man the installation through FPCON DELTA?
		DoD Std 13
		
		DoD O-2000-12-H, Chapter 22

*SO-PLN-08	**Security Forces Arming**. DoD personnel regularly engaged in law enforcement or security duties shall be armed.
	
	ARMED
	• Are all personnel who regularly perform law enforcement or security duties armed?
	• Are personnel authorized to carry firearms qualified with their applicable weapon(s)?
	  o Have all personnel issued firearms qualified at least annually?
	  o Are records of individual qualification results retained for as long as the individual possesses a firearm?
	• 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?
	
	UNARMED
	• 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?
	• 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?
	• Have all armed personnel undergone a background check to ensure no conditions exist that would prohibit the individual from being armed?
	
	USE OF FORCE
	• Has the local commander developed use of force guidance based on DoD
		DoD Std 13
		
		DoDD 5210.56, Para 4.1
		Enclosure 1, Para E1.1.4

	Directive or Service directive? • Has the General Counsel reviewed and approved the local use of force rules? • Have all armed personnel been trained on the local use of force rules? o Are personnel who have not received use of force training prohibited from carrying firearms? • 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? **CONTRACT SECURITY** • Has the local commander developed criteria for the carrying of firearms by contract security forces? • Have rules of engagement and/or use of force policy been developed for contract security forces?	DoDD 5210.56, Enclosure 2, Para E2.1.4 DoDD 5210.56, para 5.3.3

*SO-PLN-09	**Security Force Training**. Installation's Physical Security Program shall include trained Security Forces capable of performing detection, assessment, delay, and response.
	• Is there a formal training/certification program for installation security forces and augmentors?
	• Does the training program consist of initial and recurring type training?
	• At a minimum does the training consist of the following areas?
	  o Access control procedures
	  o Operation of security equipment (e.g., barriers, explosive detection equipment)
	  o Training/qualification with assigned weapons
	  o Force-on-force training
	  o Antiterrorism related training
	  o Response to critical assets and contingencies
	• Are all security force personnel performing access control procedures trained on the operation of the barrier system? Did the manufacturer conduct training?
	• Have vehicle inspection instructions been developed?
	• Have security forces and augmentors received adequate (preferably by EOD) vehicle search training?
	• Do security forces receive training on improvised explosive devices?
	• Is there a process to exercise the use of augmentees to verify availability and serve as a RAM?
	• Have security forces been trained on surveillance detection?
	• Do security forces receive training on current terrorist tactics, techniques, and procedures?
	
	TRAINING FOR CONTRACT SECURITY GUARDS
	• Does the contract stipulate training requirements?
	• Have the contract guards been trained in accordance with the task outlined in their contact?
	• Is training provided on security equipment purchased by the military installation?
	• Does the contract officer technical representative or his/her designee monitor the training of contract security guards?
		DoD Std 13
		
		DoD O-200012-H, Chapter 22

	• Do contract guards engage in joint training with the assigned military security force? • If security guards perform vehicle searches, have they been trained in the techniques approved by the installation?	
*SO-PLN-10	**Security Forces Equipment.** Installation Security Forces shall be equipped to accomplish the mission of protecting DoD assets on the installation. • Are security forces personnel equipped with appropriate weaponry as identified in the AT plan and operating instructions? • Is there a sufficient quantity/type of weapons on-hand to equip security forces and augmentees through FPCON DELTA • Are security forces equipped with individual protective equipment to respond to a CBRN event? (minimum of gloves and mask) • Does security forces have ballistic protection and is it worn as required? • Are security force augmenters similarly equipped as the security forces? • Do security forces have explosive detection equipment for use at access control points, special events, and facilities? **MILITARY WORKING DOG PROGRAM** • Do the security forces have explosive detection dogs to complement the vehicle search and RAM programs? • Is there a certification process for explosive detection dogs? • If contract dogs are used, did the installation observe/mandate the certification process for the explosive detection dogs? (determine the detection capabilities; type and probability of detection) • Are MWDs used on a recurring basis to enhance detection and deterrence? (drug and patrol dogs can be used at ACPs for deterrence) • Are MWDs integrated into the IDS (e.g., patrolling critical facilities, checking parking lots, patrolling perimeter)? • 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? • Are MWDs used on response elements to enhance internal and external intruder detection capabilities? **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? o Emergency lights and sirens o Public address systems o Search lights o Emergency road kit o First aid kit o Bio-hazard kit o Radios o Installation map	DoD Std 13 DoD O-200012-H, Chapter 22

- Post orders

COMMUNICATIONS

- Is the security forces radio net equipped with a minimum of two frequencies?
- Is the security forces radio net provided with secure voice capabilities or compliant with Data Encryption Standards (DES)? [coordinate with Emergency Management]
- Are the land mobile radio, base stations, and repeaters equipped with uninterrupted power supply?
- Are radios interoperable with other first responders, includes 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 in accordance with 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?

DURESS PROGRAM

- Is there a process to changes the duress code when compromised or at least every six months?
- Are duress codes protected as "FOR OFFICIAL USE ONLY" or higher?
- Is there a duress code for facilities and is this code known by appropriate security forces (e.g., alarm monitor, responding patrols)?
- 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?
- Are duress alarms positioned so that they can be activated without arousing suspicion?
- Are duress alarms at security post tested a minimum of daily?
- Do owner users test their own duress alarms at least quarterly?
- Are response procedures developed for duress activation?

ALTERNATE ARMING POINT

- Is there an alternate arming point for the security forces?
- Is the alternate arming point out of the potential danger area posed at the main armory?
- Are sufficient weapons stored for responding forces?
- Is there a process to access the alternate armory during non-duty hours?
- Are there written procedures for activating the alternate armory?

INSTALLATION ACCESS CONTROL		
*SO-PLN-11	**Access Control Procedures.** DoD Installations shall established 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. • Are access control procedures developed around the Design Basis Threat? • Has the installation developed written access control procedures for each FPCON? o Describes specific missions of the post o Addresses acceptable identification types o Describes emergency entry procedures o Current and covers changes that have been implemented [access control process, etc.] o Covers operation of barriers at the post o Contains gate procedures for alarm situations o Covers barment of personnel o Addresses vehicle, pedestrian, and commercial deliveries • Do procedures define who can enter the installation and the required identification? • Do access control procedures reduce access as the FPCON level increases? • Are access control measures commensurate with current higher headquarters guidance, i.e., searching commercial deliveries? • Are entry access lists required to be authenticated before being accepted by the entry controller? • Have personnel designate with escort privileges been trained on their duties and are there a maximum number of personnel an escort can escort? [Applies to facilities as well] • Is there a formal process to vouch personnel onto the installation? **ACP OPERATIONS** • Is the ACP capable of accommodating Random Antiterrorism Measures (RAMs)? • Have gates been designated for operation during all FPCONs? • Are designated gates capable of performing 100% vehicle inspections? • Has commercial gate been designated for all commercial deliveries? • Is each ACP equipped with at least two means of communications to the security control center? Consider emergency ring down. • Is the ACP capable of connecting to the installation's intranet? (Should be password protected and properly shutdown when gate is closed, consider removable hard drive)[not required but increases efficiency] • 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)	DoD Std 13 DoD O-2000.12-H, Chapter 22

	<u>ACP OVERWATCH</u>-may not be applicable at all installations. Must have a clear field of fire past the installation ACP. • Has the installation included overwatch positions in their FPCON planning? • Do the gates selected for overwatch positions have sufficient spacing for an overwatch? [coordinate with Structural Engineer] • Is the overwatch position tasked with providing observation and employing deadly force against vehicles that attempt to bypass, ram, or otherwise run through the access control point? • Is the overwatch position equipped with a weapon that can stop a vehicle by disabling it or killing the driver (at a minimum a 7.62mm machine gun)? • Has rules of engagement been developed for the overwatch position? • Have detailed standard operating procedures been developed that include command and control between the overwatch and the access control point? **<u>VEHICLE SEARCHES</u>** • Are procedures for conducting vehicle searches established? • Are security forces trained on conducting vehicle searches? • Is sustainment training developed? • Are explosive detection dogs or mechanical explosive detection equipment used? • Has standard operating procedures for use of explosive detection equipment developed? • Are drivers asked to exit vehicles? • Are vehicle searches concealed from observation?	
*SO-PLN-12	**Perimeter Security**. The installation shall develop a barrier system that establishes a perimeter to establish boundaries and deter/intimidate individuals from attempting unlawful or unauthorized entry. • Has the installation established a perimeter protection system? • Is there an active perimeter inspection/maintenance program on the installation? • 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? • Are dips, ridges, ditches, etc., or other concealment areas removed from the clear zone? • 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] • Are walls that form the perimeter boundary topped with barbed wire? **<u>FENCING</u>** • Is the fence a height of 7 feet without outriggers and 8 feet with outriggers? • Is the perimeter fence topped with concertina wire and/or outriggers (two 15-inch Y outriggers having 3 strands of barbwire each)? • Are posts, bracing, and other structure members on the inside (site side) of the fence fabric? • Is the fence fabric secured to tension wires with 12-gauge galvanized tie wire? • Is the fence fabric secured to fence posts, rails, or other anchoring materiel	DoD Std 13 DoD O-2000.12-H, Chapter 23

	with fasteners of tensile strength at least equal to the fence fabric? • 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. • 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] • Are installation warning signs posted not to exceed 100 yards apart? **UNMANNED GATES –[coordinate with Structural Engineer]** • Are gates that are not in regular use secured? [Can't be rammed open or opened by hand] • Is the bottom of the gates within 5 inches of pavement and 2 inches for soil? • Is there no more than 5 inches between the gate and gatepost? • Are gates secured with Type II or III Secondary padlock if not equipped with electric locks? • Are keys to perimeter gates restricted to the security forces? • 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?	
ELECTRONIC SECURITY SYSTEM (ESS)		
*SO-PLN-13	**Electronic Security System (ESS)**. Installation Physical Security Program shall include a security system capable of protecting DoD Assets. • Does the physical security system perform the following functions: o Threat Detection o Threat Annunciation o Threat Classification and Assessment o Threat Delay **THREAT DETECTION -**The threat detection system should provide as early as possible detection to increase the opportunities to protect Do assets and minimize the impact of terrorist acts against DoD personnel, materiel, and facilities. • Were the following considerations used to determine the appropriate surveillance systems performance and selection: o Seasonal and/or ambient weather conditions o The type of background against which surveillance systems are attempting to operate. (Can effect sensitivity) o 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)	DoD Std 13 DoD O-2000.12-H, Chapter 22

	• Does the installed alarm sensor system perform the following functions? o Line of detection on a fence ▪ Detect cutting ▪ Detect climbing on the fence ▪ Detect lifting the fence o Line of detection at the area perimeter, in a clear zone, airfield taxi gap, or around individual resources o Detect walking ▪ Detect running ▪ Detect rolling ▪ Detect crawling across ▪ Detect jumping through the line of detection o Line of detection at a facility ▪ Must detect intrusion attempts through likely avenues ▪ Intrusion through doors ▪ Intrusion through windows ▪ Intrusion through walls ▪ Instruction through roof or vents	

*SO-PLN-13A	**THREAT ANNUNCIATION-** The threat detected by the security system must be reported to a central location where security forces can be dispatched. **CONSTRUCTION OF THE CONTROL CENTER** • Is the system located in a restricted area and closed off from public view? • Is the facility constructed with suitable ventilation, heating, and air conditioning? • 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? • Is there one-way glass panel, CCTV coverage, or similar viewing device to identify personnel requesting entry? • Is the main terminal for the Land Mobile Radio (LMR) base station and landline system installed in the control center? • Is the control center equipped with landline communications with each fixed, permanent, static access control post, command post, control tower, fire department, subordinate C3 facilities, flightline maintenance, and munitions control, as applicable? **ALARM MONITORING STATION** • Is there an annunciation capability where security forces can be immediately dispatched? • Are alarms audible and visual? • Are all alarms recorded? • How are systems malfunctions recorded and reported? • Has a nuisance rate been established for the system? What is the nuisance rate (e.g., per 24-hour per sensor field, etc.)? • Has the installation command structure determined what constitutes catastrophic, major, and partial failure of the IDS? o Are there contingency plans/compensatory measures for each type of failure? • Has a maintenance response priority been established for each type of failure? • Is there a redundant capability for this system? • Are the data transmission lines secured?	DoD Std 13 DoD O-2000.12-H, Chapter 22.5.5

*SO-PLN-13B	**THREAT CLASSIFICATION AND ASSESSMENT -** The physical security system should be able to determine whether the alarm is real or false, and if the intrusion is hostile or benign. • Is a CCTV system employed to assist in the alarm assessment role? • Is the CCTV system connected as a slave to the IDS? (Video interfaced for alarm assessment camera call-up) • Does the security system include a night viewing device, an imaging infrared device, human intervention or other method of assist in classifying the threat? • Is there a video recording capability for forensics? (Digital is preferred) • Is lighting adequate to assess the threat? (6 to 1 Light to Dark Ratio) • Is CCTV coverage provided for the following interior areas: o Card reader door assessment o Emergency exit door assessment o Surveillance of lobbies, entrances, corridors, and open areas o Is fiber optic (preferred type) used as the transmission system from the CCTV to the central-monitoring station? **THREAT DELAY-** The physical security system should have a built in delay system that provides the minimum delay time on any path to the protected area. • 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) • 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? • Does the delay system meet the minimum delay requirement established by the installation? • Does the delay system meet the three requirements for a delay system: o Facilitate definitive threat classification ad assessment o Facilitate response by security forces o Facilitate evacuation of protected DOD assets if evacuation is the most appropriate, cost-effective AT remedy	DoD Std 13 DoD O-2000.12-H, Chapter 22.4.3

SO-PLN-14	**Installation Lighting.** The installation lighting system should enable security forces to observe activities around or inside an installation without disclosing their presence. • 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? • Does the level of lighting take into consideration the contrast between the intruder and the background? • Is the installation lighting system comprised of the following types if lighting: • Continuous lighting which includes glare projection and controlled lighting • Standby lighting – used when suspicious activity is detected or suspected • Emergency lighting • Motion activated lighting • Is lighting assured through engineering? (Coordinate with Infrastructure Engineer) • 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)	DoD Std 13 DoD O-2000.12-H, Chapter 22.6
*SO-PLN-15	**Bomb Threat Plans**. The installation shall develop plans/procedures to respond to a bomb threat. • Has the installation developed a bomb threat response plan? • Does the installation bomb threat response plan include the following processes? • Bomb threat mitigation • Notification and evacuation procedures • Search procedures • Does the installation AT Plan identify requirements for facility-specific bomb threat plans (i.e., a template)? • Has the bomb threat response plan been reviewed by EOD? • What is the response time for EOD to arrive? (Coordinate with EM) • If no organic EOD capabilities exist, are there agreements to get the support from the local/host-government authorities? • What are the interim measures that are implemented until arrival of EOD?	DoD Std 7 DoD O-2000.12-H, AP3. Tab A

MAIL HANDLING PROCEDURES		
*SO-PLN-16	**Mail Handling Procedures**. Installations shall develop preventative measures against the introduction of explosives and chemical or biological laden mail from entering the installation's mail handling system. • 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] • If mail is screened, is there a process to verify integrity of the mail from point of inspection to delivery? • If mail is not screened, has the installation developed a process and procured required equipment to perform screening? • Has the installation/facility developed formal, site-specific, procedures for explosives and chemical/biological suspicious mail? [Separate and distinct procedures] • Are all personnel who handle mail trained on these procedures? • Are training aids available in the mailroom? • Are mail handlers trained on the mail screening devices? • Is there a process to conduct routine testing of the mail screening devices, i.e., sending through a simulated threat? • Is the mailroom equipped with the following equipment for chemical/biological incidents: o Gloves (avoid powder coated gloves) o Large sealable bags for isolating suspicious mail and discarding all clothing worn during contact with contaminants o Change of clothing o Surgical mask or protective mask (commercial mask are available) • Are mail handlers informed and trained on how to shutdown the ventilation system in case of airborne contaminants? • Is the mail handling plan exercised? [coordinate with the Infrastructure Engineer] • Are there plans for a central mail delivery/inspection center during increased FPCON?	DoD Std 13 DoD O-2000.12-H, AP3, Tab C
AT MEASURES FOR HIGH-RISK PERSONNEL (HRP)		
SO-PLN-17	**High-Risk Personnel**. 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. • Are there any officially (through Military Service channels) designated HRP or HRB assigned to the installation? • Is a process to conduct a PSVA on HRPs established • Has the installation developed protective measures for HRPs? • Are the protective measures promulgated in the AT Plan? • Is there a process to review HRP security measures within 60 days of to the Terrorist Threat Level? • Are protective measures tied to the FPCON system?	DoD Std 16 Strategic Goal 3D

	HRP/HRB TRAINING • Has the installation established required training for HRP/HRB? • 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 whom are entitled to additional measures as a result of their position. [OCONUS] • Is there a process to notify Military Services of personnel and their family members requiring formal HRP training before assignment? • 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)?	
SO-PLN-18	**Office Security**. 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. • Has a vulnerability assessment of the office area been performed? • Are the following security enhancements selectively implemented in the office of HRPs and senior executives? • Installation of surveillance systems • Access points away from the office entrance • Duress systems within the office • Install vehicle barriers and realign roadways to eliminate straight, level stretches of road in excess of 50 meters in length • Increase concentric rings of fences, Jersey barricades, planters, bollards, and vehicle and/or personnel barriers • Access control areas, supplemented by fire doors and/or security doors kept in close condition, between the entrance to the building housing executives offices and executive office area itself • Confuse, camouflage, and deceive observers by hiding designee's location • Consider relocating executives to buildings not usually associated with office activities, e.g., barracks, motor pool, R & D facilities (Note: this may be included as an FPCON measure) • Add executive style, decorative lighting and window treatment to several different office buildings to minimize differences in external appearances • Replace standard doors and door frames leading into the protected office with high security doors and doorframes • 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 • Limit public available information, i.e., official biographies to the bare minimum **SAFE HAVEN** - Personnel requiring a high level of protection in high threat areas should include a **safe haven**. The safe have should be the inner most layer of protection within a physical security system. • 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?	DoD Std 16 DoD O-2000.12-H, Chapter 21

	• Was the response time by the security force factored into the required delay? • Is the safe haven large enough to accommodate the personnel intended to use the location? • Is it free of windows and vents that could allow introduction of contaminants? • Is the safe haven equipped at a minimum with the following items: o Food o Water o Medical supplies o Communications	
SO-PLN-19	**Office Security Procedures.** Installations should implement special considerations for secretaries and executive assistants who also perform collateral security duties for high-risk personnel. • Are the following security considerations provided for the secretary and executive assistant? • Installation of physical barriers such as electromagnetically operated doors to separate offices of the high-risk personnel or senior executive from other offices • Installation of a silent duress alarm button with a signal terminating at the security department • 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) • Prohibition on issuing information to unknown callers • Storage of first aid kit and fire extinguisher in the office area • Posted procedures for handling threatening calls • Prohibitions on accepting packages from strangers • Mail handing procedures • Limited distribution and visibility of travel itineraries and schedules of senior officials	DoD Std 16 DoD O-2000.12-H, Chapter 21
SO-PLN-20	**Protective Security Details (PSD)**. 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. • Is the level of protection for the protected appropriate for the threat? • Do personnel assigned PSDs meet Service regulation requirements? • Are travel itineraries reviewed by the PSDs to ensure protection of routes and times? • Is there a formal selection process for PSD members? • Is there a training program for PSD members? • Has an operating instruction been developed for PSD operations? • 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? • Duress signals • Call-in • Carrying duress notes written on money • Duress alarms and/or radio links	DoD Std 16 DoD O-2000.12-H, Chapter 21, C21.10 and APP 15

	• Varying routes • Clothing changes • What to do if taken captive • Contact with police • 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?	
AT MEASURES FOR LOGISTICS and CONTRACTING		
*SO-PLN-21	**Logistics and Contracting**. 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. • Has the installation developed AT measures for the contracting office to include in applicable contracts? • Are Combatant Commander AOR and/or country specific AT security guidance incorporated into the installation's process, if developed? • Is there a process to ensure that contracts comply with the AT Provisions in the Defense Federal Acquisition Regulation Supplement (DFARS)? • Is the ATO coordinating contracting requirements with the contracting officer and the legal office? • Are contracting security requirements based on the individual threat concerns and arrangements with the host nation? • Are contracting procedures referenced or included in the AT Plan? • Is the commander's guidance for the AT security criteria applied as a baseline for all contracts? • Are contracts/contractor included during the commander's AT risk assessment process? • Is the contractor's performance evaluated when future contracts are awarded?	DoD Std 18 DoD O-2000.12-H, AP8.1.1. Strategic Goal 2D
SO-PLN-22	**Background Investigation for Contractors.** 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 of or provide services related to mail, supplies, food, water, or other material and equipment for use by DoD personnel. • Is there a process to conduct background investigations on contractors and sub-contractors? • Does the installation have a process to verify that background investigations have been conducted? • Do background investigations include husbanding agents and crews on contracted ships, planes, and overland vehicles? • Are contractor personnel screening requirements met before the start of the contract? • If screening is not completed, is there a process to escort personnel until screening is completed? • 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	DoD Std 18

	security measures are in place?	
SO-PLN-23	**Site-specific Risk Mitigation**. 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? • Are contractors provided security briefs on circulation control? • Have risk mitigation measures been developed for the installation? • Are contract security requirements incorporated into the local FPCON measures? • Are special security concerns listed in the contract security requirements? o Frequent, random patrols o Inspections o Spot-checks o Food, water, and petroleum distribution sites o Provide training for reporting suspicious activity • Does the installation have a process to retrieve access media from employees of expired contracts? o Is there a process to immediately retrieve access media for terminated contractors? • 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]	DoD Std 18
AT MEASURES FOR CRITICAL ASSET SECUIRTY		
*SO-PLN-24	**Critical Asset Security**. 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. • Have security measures been developed for assets identified on the Mission-essential and/or vulnerable areas (MEVA) or Critical Asset list? **ASSESSMENT OF CRITICAL FACILITIES** • What is the design basis threat (weapons and tactics) for which the asset is to be assessed? • Are security measures based on threat, criticality, and vulnerability? • 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) • Are drawings of the facility controlled to prevent the disclosure of sensitive information? **PLANNING** • Does the facility's Physical Security or AT Plan complement the installation's AT Plan and contain the minimum requirements outlined in the plan? • Has the facility's Physical Security Plan been reviewed by the installation ATO? • Is there a representative who attends the installation's ATWG (if tenant on the installation)? • Does the facility have physical security plans that explain, at a minimum, how the facility will:	DoD Std 19 Strategic Goal 2D

- Transition through each FPCON
- Participate in the installation's RAM program
- Control personnel access
- Vehicle access if applicable
- Implement barrier plans (coordinated with ATO)
- Bomb threat plans

- Are personnel identified to protect these assets during increased threats?

PERIMETER / EXTERIOR

- Are there any public access vantage points that allow potential aggressors to observe and target people or other assets in or around the building?
- Are there any signs that identify the criticality or sensitivity of the facility?
- If there are commercial transportation nodes closed to the facility, are there any procedures in place to prohibit stopping adjacent to the facility?
- 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?
- Are electrical and mechanical equipment provided enclosures to prevent placement and concealment of explosive devices?
- If parking garages are located underneath the facility, is access controlled for pedestrians and vehicles?
- Is sufficient lighting provided for vehicular and pedestrian entrances, and perimeter? [check backup power availability]
- Does perimeter lighting provide continuous lighting on both sides of the perimeter barriers?
- Is lighting sufficient enough to support CCTV (if installed) operations and other surveillance?

ACCESS CONTROL FOR CRITICAL FACILITIES

- Has an access control system/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? **FACILITY BOMB THREAT PLAN** • Have written bomb threat procedures been developed? • Are the procedures based on the installation's requirements? • Do procedures identify primary and alternate rally points? o Identify leadership and accountability procedures? • Does the facility have a unique alert tone (separate from the fire alarm) to evacuate the facility? • Are new employees or building occupants trained on the bomb threat response procedures? • If a billeting area, are occupants provided information on the bomb threat plan? • Have search team members been identified and trained on search procedures? • Do all personnel have the installation's version of the current bomb data collection sheet? • Has the installation ATO and/or EOD reviewed the bomb threat plan? • Are plans coordinated with adjacent facilities to avoid confusion during evacuation? • Is there an established frequency to exercise the bomb threat plan? • Are acceptable mail and parcel handling procedures being followed to include screening, delivery, and response for expected explosive devices? • Are mail handlers properly trained in identifying mail and parcel bombs and exercises are being conducted to ensure personnel remain trained and alert?	
SO-PLN-25	**Off-Installation Critical Assets.** 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] • Has the commander coordinated for the protection of non-DoD critical assets? • Do Security Forces coordinate with local law enforcement to provide security coverage of these assets?	DoD Std 19 Strategic Goal 2D

	AT MEASURES FOR OFF-INSTALLATION FACILITIES, HOUSING, AND ACTIVITIES	
*SO-PLN-26	**Off-Installation facilities/activities**. Installation commanders shall develop in their overall AT programs specific AT measures for off-installation facilities, housing, and activities. • Has the commander developed AT measures for the following off-installation activities: o Facilities (physical security measures) o Housing (guidance for selection/physical security measures) o Transportation Services (planning and route analysis) o Daycare centers (physical security measures) o Activities used by or involving mass-gathering of DoD personnel and their family members • 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? • Based on the physical security surveys, does the installation have procedures to provide AT recommendations to residents and facility owners? • 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? • Are route maps of residences maintained at a 24 hr 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? • Do unit AT plans include current residence location information for all unit members residing off-installation? • Do incident response plans include measures for off-installation personnel (personnel warning system)? **HRPs RESIDING OFF-INSTALLATION** • Has a risk assessment been conducted to determine the level of security required for residents of high-risk personnel? • Is there a site selection criteria for HRP housing? • Has a vulnerability assessment of the residence been performed?	DoD Std 15 DoD O-2000.12-H, Chapter 22 Strategic Goal 2F
TERRORIST INCIDENT RESPONSE / TERRORIST CONSEQUENCE MANAGEMENT [coordinated with Emergency Management]		
SO-PLN-27	**Terrorism Consequence Management**. The installation commander shall develop a crisis management plan to respond to a terrorist incident. • Have the following items been included in crisis management planning? o Are special threat plans and physical security plans mutually supportive? o Does the special threat plan include the threats identified in the threat statements of higher headquarters? o Does the plan provide for a response for each phase of antiterrorism activity (e.g., initial response, negotiation, assault)? o Does the plan take into consideration the movement from various	DoD Std 20 DoD O-2000-12-H, Chapters 11 and 12, AP5 Strategic Goal 2D

	locations, including commercial airports, of civilian and military advisory personnel with military transportation assets? o 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)? o Does the plan make provisions for paying civilian employees overtime if they are involved in a special threat situation? **REACTION FORCE TRAINING** • 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)? • 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? • Has the force been trained and exercised under realistic conditions? • Has the reaction force been tested quarterly (alert procedures, response time, overall preparedness)? • Has a hostage negotiations team been identified? Has the negotiation team been trained and exercised under realistic conditions? • Does plan include the potential for an interpreter?	
SO-PLN-28	**Terrorism Incident Response**. Installation commanders shall develop terrorist incident response measures consistent with the DoD O-2000.12-H and include these measures in the overall AT Plan. • Has the installation developed terrorist incident response measures and included them in the AT Plan? (coordinate with Emergency Management/CBRNE) • Has the installation identified required support for overwhelming incidents? • Are security forces identified for response to terrorist incidents?	DoD Std 20 DoD O-2000-12-H, Chapters 11 and 12, AP5 Strategic Goal 2D

3. ANTITERRORISM TRAINING AND EXERCISES		
SO-TE-01	**AT Training and Exercises**. 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. • Is training provided to the security forces to conduct all phases of the installation's Physical Security Program? • Are training records maintained? • Are exercises conducted with the local responders?	DoD Std 23 Strategic Goal 3F
SO-TE-02	**Pre-deployment Training.** 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). • Does AT training include measurable standards? • Does training for deploying forces include deterrence, response standards, deterrence-specific tactics, techniques, and procedures? • Is training for deploying forces documented? • Is training designed to meet gaining Commanders requirements? • Is AT training incorporated into unit level training plans and pre-deployment exercises? • Are deploying members trained on local security procedures at the deployed location? • Are terrorist scenarios included in the pre-deployment training? • Are personnel involved in law enforcement / security trained in hostile intent decision-making? • Are deployed commanders trained in hostile intent decision-making?	DoD Std 23 Strategic Goal 3B
*SO-TE-03	**Formal AT Training**. 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. • Is there a process to ensure personnel received appropriate AT training? • Is there a documentation process for accomplished training? • Is there a process to ensure HRPs receive appropriate training?	DoD Std 24 Strategic Goal 3E
*SO-TE-04	**Reporting AT Training Deficiencies.** 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. • Is there a process to screen records of incoming personnel for AT training? • Is there a process to ensure personnel who have not received AT training are provided the training as soon as practical? • What is the process to report receipt of untrained personnel through the chain of command?	DoD Std 24 Strategic Goal 3B

*SO-TE-05	**Level I AT Awareness Training.** Installation commanders shall ensure that Level I AT Awareness training adheres to the minimum requirements listed in Table E3.T1 of DoDI 2000.16. • Is Level I AT Awareness training provided in accordance with the curriculum described in DoDI 2000.16? • Is individual awareness of terrorism threat sufficient for threat environment/mission? • Are localized individual protective measures included as part of the Level I training? • Is there a method of tracking training to ensure all personnel have received the required training? • Is there a process to ensure all personnel annually receive Level I AT Awareness Training? **FAMILY MEMBERS** • Are family members provided Level I AT Awareness training for official travel? • Are family members encouraged to complete Level I AT Awareness training when traveling on other than official travel outside CONUS or areas where the threat level is Moderate or higher? **CONTRACTORS** • Is the requirement to attend Level I included in contracts? • Are contractors afforded the opportunity to attend Level I training? **Host-Nation/Third Country National** • Does Level I AT Awareness Training include local nationals and third country nationals? • Is training provided to local nationals and Third Country Nationals in their native language?	DoD Std 25 JP 3-07.2 Strategic Goal 3B
*SO-TE-06	**Level I Instructors**. Installation commanders shall designate in writing all individuals qualified to administer Level I AT Awareness Training. • Does the ATO maintain the list of those personnel qualified to administer Level I AT Awareness Training? • Are instructors certified using one of the following methods? o Completion of a formal Military Service-approved Level II ATO Training Course of Instruction whether resident or through a mobile training team o Completion of a DoD-sponsored and certified computer or web-based distance learning instruction course for Level II ATO Training. o 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. • 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?	DoD Std 25

*SO-TE-07	**ATO Level II Training**. Installation Antiterrorism Officers shall complete an approved Level II ATO Training Course. • Has the ATO completed an approved Level II ATO Training Course? • Has the ATO accomplished refresher training if it has been three years since attending Level II?	DoD Std 26
*SO-TE-08	**AOR-Specific Training**. 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. • Is there a written process to ensure all personnel meet the gaining COCOM's requirements? • Is there a mechanism used to ensure PCSing personnel receive the AOR-specific brief within 3 months of departure? • Is AOR-specific requirements fulfilled for deployments? • Does the installation ensure intra-theater transiting units receive detailed threat information covering travel routes and sites that will be visited by the unit?	DoD Std 29 Strategic Goal 3B
4. AT RESOURCE APPLICATION		
*SO-RA-01	AT Resource Application Process Installation commander shall identify AT resource requirements use the DoD-approved methodology for documenting and prioritizing AT resource requirements. • Does the installation's AT Resourcing process use the risk analysis (criticality, threat, and vulnerability) products for resource determination? • Is there a resource justification / prioritization process that incorporates the following? o Threat o Asset Criticality o Asset Vulnerability o Current AT effectiveness o Impact on Plan / Programs o Mitigation Measures o Commander's Risk • Is the prioritization focused on the most critical and important needs first? o Resources necessary to meet minimal security requirements and to adhere to DoD Service directives, standards, instructions, or regulations. o Resources required to mitigate a major or a high risk situation • Is the ATWG involved in the prioritization of resource requirements? • Are the projected resource requirements: o Affordable o Supportable o Reduce risk o Provide a high or moderate impact on the program to achieve the objectives identified in the AT Plan • Does the installation have an acquisition strategy to obtain funding sources? • Does resource cost include all life-cycle cost (manpower needs, logistics / maintenance, replacement cost)? o Are AT resource requirements matched against other organization	DoD Std 30 Strategic Goal 4C

	unfunded or funded requirements to determine if an internal reallocation of funding is appropriate and possible? • Are unfunded requirements entered into the Core Vulnerability Assessment Management Program (CVAMP)?	
SO-RA-02	**CbT-RIF Submission**. The installation commander shall have procedures to adhere to the HHQ's CbT-RIF submissions. • 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) • Is there a plan to obligate funding within 90-days of receipt, if CbT-RIF funds have been approved? • 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] • Are CbT-RIF submissions entered into CVAMP?	DoD Std 30 CJCSI 5260.01D Strategic Goal 4B
*SO-RA-03	**AT Technologies.** The installation commanders shall incorporate AT technologies into their AT program to enhance AT readiness, emergency preparedness, and improve CBRN-related protective measures, specifically in the following categories: • Detecting and defeating improvised explosive devices • Investigative / Forensics Support • Physical Security • Protecting Critical Infrastructure • Personnel protection • Training technology development • Does the installation use technology to mitigate vulnerabilities where applicable? o Does the installation use the Antiterrorism Enterprise Portal (ATEP) to research available and tested technology?	DoD Std 13 Strategic Goal 4E
5. COMPREHENSIVE AT PROGRAM REVIEW		
*SO-PR-01	**Comprehensive Program Review**. 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. • Has the installation defined a process to conduct program reviews?	DoD Std 31 DoD O-2000.12-H Chapter 15; AP1

	• Who has been designated to conduct the program reviews? • Has a tool (checklist, etc.) been developed for assessors? • Does the assessment tool contain command-specific assessment items? • Does the review process conform to requirements of Std 31 of DoDI 2000.16? • 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? • Is there a process to conduct program reviews whenever there is a significant change in threat, vulnerabilities, or asset criticality necessitate? • Are tenants included in the program review? **PRE-DEPLOYMENT PROGRAM REVIEW** • Are program reviews conducted to ensure deploying units have viable AT programs and executable AT plans?	Strategic Goal 5C

	ADDITIONAL PHYSICAL SECURITY BENCHMARKS **PORT SECURITY**	
*SO-PS-01	**Port Security Plan.** 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) • Does Port Security Plan should address: • Policies • Plans • Procedures • Systems and equipment that will: • Detect • Assess and classify threats • Communicate warnings and threat assessment information • Delay adversaries and provide for timely, effective response to a waterborne threat • Barriers, lighting, CCTV and intrusion detection systems • Consideration to potential terrorist targets • Restricted areas • Use of patrol boats • Protection for sea approach choke points • Considers off-port observation points capable of observing port activities and the transit area	DoD Std 7 DoD 5200.8-R DoD O-2000.12-H, AP 4

SO-PS-02	**Physical Security System**. Waterside physical security system should include barriers to establish a boundary, isolate activities, and discourage visitors, and impede passage by boat or swimmer. [coordinate with team Structural Engineer] • Is there a barrier plan to complement waterside security? • Are barriers placed far enough from the assets to provide adequate protection based upon the design basis threat? • Do selected barriers provide surface and subsurface protection? • Are patrol boats incorporated into the barrier plan? • Are boats prohibited/prevented from coming within 500 meters of a DoD asset? **SURVEILLANCE** - 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? • Does the facility have an external surveillance program? • Does the surveillance program extend beyond the capability of the waterborne threat? • Are areas under surveillance included in the security zone? • Does the surveillance program include central radar monitoring waterside area (warship radar, shipping/harbor control radar, expedient use of mast mounted radar on-shore). Lookouts posted topside on ships with night vision devices? • Does nighttime surveillance include the use of radar? • Are acoustic underwater sensors employed for surveillance purposes? • In high threat areas, is aerial surveillance employed? **SECURITY ZONE** - 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. • Has an appropriate Security Zone been established? • Is the Security Zone based upon the threat assessment? • Has a reaction zone been established within the Security Zone? • Is the Security Zone developed to include multiple ships when present? • Have navigational aids mounted on structures in shallow water included in the security zone (may also include airfield navigational aids in bays and rivers)? • Has the Security Zone been coordinated with the local/host government authorities? • Are local/host nation authorities involved in the enforcement of the Security Zone? • Is the Security Zone marked on navigational maps as well as aeronautical when there is a "No Fly Zone"? • Has a "No Fly Zone" been coordinated/established through the Transportation Security Administration (TSA), or host-government authorities? • Is the Security Zone prominently marked on the waterside?	DoD Std 13 DoD O-2000.12-H, AP17.3 DoD O-2000-12-H, C22.14.4 DoD 5200 8-R

	Perimeter Security. 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] • Has the threat assessment identified the threat of a standoff weapons attack from the water? [coordinate with Terrorist Operations] • Does the security perimeter extend out beyond the distance of the weapon capability? • Is the perimeter secured to prevent the threat from gaining access into the security perimeter to launch the standoff weapons attack? **CLASSIFICATION/ASSESSMENT** • Is there a process to classify the threat once an intruder has been detected? **RESPONSE** • Have lesson plans been developed to train personnel responsible for waterside security? • Is other law enforcement type training provided (i.e., U.S. Coast Guard, Marine Patrols)? • Have security forces (i.e., organic security forces, U.S. Coast Guard, state or local police, host-government forces if overseas) identified to respond to intrusions in the Security Zone?	DoD Std 13 DoD O-2000-12-H, C22.14.4, AP 17
SO-PS-03	**Coordination for Waterside Security**. Coordination shall be conducted with federal, state, and local agencies, law enforcement and security agencies, and port stakeholders. • Have support agreements been developed with the local law enforcement and other port authorities for support during terrorist incidents? • Have the provision of the agreements been validated through a practical exercise? • Is joint training conducted between all responding forces?	DoD Std 8 DoD 5200 8-R
SO-PS-04	**Ships outside of Homeport.** 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. • Is there a process to ensure all departing ships have an approved in-port force protection plan? • Are measures to be taken consistent with local rules, regulations, SOFA and the approved in-port force protection plan? [must identify the deployed location]	DoD Std 7 DoD O-2000.12-H, Chapter 22, AP3.2 .1.2

SO-PS-05	**Deployed Ships.** Commanders shall implement a security watch for deployed ships that provide safeguards from sabotage, terrorism, civil disturbance, danger, or compromise? • Has the commander established a security watch? • Is an Officer of the Deck (ODO) or equivalent appointed and has the responsibility for posting all security watches/sentries? • Are all watch standers bearing arms properly qualified? • Is there a communications plan for watch standers? • Are rules of engagement established? • Are watch standers trained in hostile decision-making? • Is there a demarcation zone that identifies the area where watch standers may engage targets? • 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? • Are watch standers provided written access control procedures to board the ship? Personnel should be denied access until cleared by the ODO.	DoD Std 13 DoD O-2000.12-H, Chapter 22, AP3.2 .1.3
SO-PS-06	**Deliveries**. Material brought aboard ship shall be randomly inspected by watch standers, 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) • Is there a process to randomly inspect materiel prior to being brought on board? • Are personnel performing these inspections trained in search techniques? • Is there a process to incorporate technology and/or explosive detection dogs into the random inspection process?	DoD Std 13 DoD O-2000.12-H, Chapter 22, AP3.2 .1.5
SO-PS-07	**Deploying Ships.** Deploying ships shall accomplish pre-deployment procedures. (also use pre-deployment VA and Training Benchmarks) • Do pre-port procedures include the following? o Obtaining a current threat assessment from the local NCIS representative o Senior commander issues security requirements for all ships o Briefing crew on threat, security precautions, recall procedures, and ship's Self Defense Force (SDF) duties o Brief security forces, brief threat specifics, review of rules of engagement or use of force policies, security assignments, and responsibilities o Brief beach guards and shore patrols on threats and review special procedures applicable to the specific port visit including pier and/or fleet landing security and access control procedures o When operating under FPCON BRAVO, in non-Navy ports, or a threat to a specific ship is received, use a MWD and divers to conduct a search of the pier prior to the ship's arrival, when available	DoD Std 13 DoD O-2000.12-H, Chapter 22, AP3.2 .1.6

SO-PS-08	**Contracting**. 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) • Is there a process to ensure trustworthiness of non-DoD personnel supporting ship operations? • Does the process include follow-up investigations? • Is this process incorporated into the contract?	DoD Std 13 DoD O-2000.12-H, Chapter 22, AP3.2
ADDITIONAL PHYSICAL SECURITY BENCHMARKS – AIRFIELD SECURITY		
SO-AS-01	**Airfield Security Plan.** The AT Plan shall include plans for protection of airfields located on the installation. (reference AT Planning Benchmarks) • Does the plan address: o Access control o Intrusion detection systems o Barrier plan o Airfield-specific FPCON measures o Security response o Expanded Security Operations • Does the airfield security plan incorporate support identified in the installation AT plan?	DoD Std 7 DoD 5200 8 R DoD O -2000.12-H, Chapter 22, C22.12

SO-AS-02	**Physical Security System.** Installation commander shall provide protection of DoD assets located on installation airfields.
	• Does airfield security consist of the following components?
	  o Multiple internal security perimeters
	  o Hardening of selected buildings against terrorist attacks
	  o Hardening of petroleum storage
	  o Aircrew facilities
	  o Maintenance facilities
	  o Other collocated facilities
	• Is airfield security planning in accordance with applicable HHQ requirements?
	• Are runway and taxiways included in the protection scheme, to include the utilities that may be buried beneath them? [coordinate with Infrastructure Engineer]
	• Are aircraft in maintenance provided appropriate protection, security forces or maintenance personnel?
	
	PARKING AREA/ACCESS CONTROL
	• Are aircraft parked within a restricted/controlled area?
	• Is there a separate airfield perimeter fence (requirement depends on type of resource and installation perimeter)?
	• Is positive access control provided for sensitive airfields (e.g., Priority Level resources, alert aircraft, and DV aircraft)?
	• Is there an identification system that allows access to the flightline for vehicles and personnel?
	• Are barriers in place to control vehicle access?
	• Are high-speed approaches mitigated?
	• Are access control points randomly manned?
	• Do security forces conduct random credential checks in the flightline area?
	• Are parking areas prominently marked with warning signs?
	• Is there a process to limit vehicle access points for increased threats?
	
	INTRUSION DETECTION SYSTEM (IDS) – use ESS Benchmarks
	• Are multiple layers of IDS used on the airfield (line detectors, motion detectors mounted on fences and seismic or acoustic sensors sown in patterns)?
	• Are airfield electronics protected (i.e., devices to support aircraft takeoffs and landings in all weather and visibility conditions)?
	• Is beyond-the-perimeter surveillance incorporated into the airfield security planning?
	• Are special aircraft equipped with IDS?
		DoD Std 13
		
		DoD 5200 8-R, Chapter 4
		
		DoD O-2000.12-H, Chapter 22, C22.12

SO-AS-03	**Man-Portable Air Defense System (MANPAD).** Procedures to mitigate MANPAD threats should be developed. • Has a MANPAD Risk Assessment been conducted to identify areas vulnerable to a MANPAD threat (possible launch sites)? • Has contingency plans been developed to respond to MANPAD threats? • Does the AT Plan address the following considerations: o 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. o Incorporates current airfield threat and security assessments, especially for deployments o Varying arrival and departure times of aircraft. o Randomly changing approach and departure routes as a deterrent (in accordance with current TSA guidelines) o Limiting or discontinuing use of landing lights within identified threat zones o For high threat areas—coordinate and develop plans for engine running offloads to minimize ground time • 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? • Has observation post on and off base been designated? o Off-base observation post should be coordinated with local authorities **COUNTERMEASURES** • Have MANPAD defense been included in the AT Plan and does this defense includes the following: o Increased physical presence at prime launches sites. Visual observations of security teams is a strong deterrent o Focused and random patrols of vulnerable areas. Random patrols should be part of the installation random AT measures program o Implementation of technical surveillance of vulnerable areas to include both launch sites and potential targets o Ensuring personnel are educated on MANPAD threat (to include component recognition), areas of vulnerability, and reaction plans. ▪ MANPAD awareness training for security force personnel and local/host nation law enforcement ▪ MANPAD awareness program for neighborhood watch groups and local businesses/installation facilities in close proximity to airfields or along flight paths o 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 • Developing and exercising contingency plans for responding to an incident of a MANPAD threat	DoD Std 13 DoD 5200 8-R DoD O-2000.12-H, Chapter 22, C22.13

SO-AS-04	**Deployed Aircraft.** Commanders shall provide protection for deployed aircraft and crews. [Refer to pre-deployment VA and Training Benchmarks] • Are the following procedures implemented for deployed aircraft? o Assign an ATO o Assess threat for all locations the aircraft(s) and crews will visit o Determine availability of security forces at all stops o Determine detection capability at the deployed location o Determine access control procedures at deployed location o Determine response capability for enroute stops and those in place at the final destination o Protect deployment itinerary o Aircraft commander will pre-plan enroute security o 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) o 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) o Coordinate security force requirements if aircraft deploys security forces (e.g., weapons storage, communications, vehicles, security equipment) o Plan for deployed sensors o Plan security for housing deployed personnel to include transportation to and from airfield?	DoD Std 13 DoD O-2000.12-H Chapter 22

Annex C
Structural Engineering Benchmarks

1. AT RISK MANAGEMENT		
	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, employ countermeasures, and mitigate and recover from the effects of a terrorist incident attack.	

*SE-RM-01	**Terrorism Threat Assessment**. A Terrorist Threat Assessment shall be completed that identifies the full range of known or estimated terrorist capabilities. [coordinate with Terrorist Operations]
	• Has the installation integrated a Design Basis Threat into their planning process?
	  o Has a Design Basis Threat (DBT) been developed by the Combatant Commander?
	  o If not, has the commander developed a local DBT?
	  o Is the Unified Facility Criteria (UFC) used in lieu of designated DBT?
	• Is the DBT validated by the local Threat Assessment?
	• Are the engineers cognizant of the installation's DBT and use it in their planning?
		DoD Std 4
		
		JP 3-07.2, Ch. III, VI, & AP B
		
		DoD O-2000.12-H, Chapters 5, 24
		
		DoD O-2000.12-P,
		
		Strategic Goal 1E
		
		UFC 4-010-01; 4-010-02; 4-020-01FA
		
		TM 5-853-1

*SE-RM-02	**Terrorism Criticality Assessment**. Establish a Criticality Assessment (CA) process to identify, classify, and prioritize mission-essential assets, resources, and personnel critical to DoD mission success. Criticality Assessments shall also be conducted for non-mission essential assets such as high-population facilities, mass gathering activities, and any other facility, equipment, service, or resource deemed important by the commander. Note: Determine the types of structures identified on the critical asset list and determine if the list needs to be expanded based upon the critical asset criteria in DoD Std 5. [Report any additions to the CA to the Terrorist Operations Specialist] • Does the criticality assessment identify high-population facilities and mass gathering activities, to include tenants? • Is the engineering department familiar with the prioritization of structures and do their plans match the critical asset list, e.g., building restoration, priority work orders, etc.	DoD Std 5 DoD O-2000.12-H Chapters 7, 8, 9 Strategic Goal 1F UFC 4-010-01 & 4-010-02

*SE-RM-03	**Terrorism Vulnerability Assessment**. The Installation Commander shall perform a vulnerability assessment (VA) to provide a vulnerability-based analysis of personnel and critical resources susceptible to terrorist attack. The assessment shall include sea and air ports of embarkation / debarkation; movement routes (sea, air, ground, and rail); and assembly, staging, reception, and final bed-down locations in support of any battalion, squadron, ship, or equivalent operational deployment; similar sized in-transit movement or training exercise; and any movement or shipment of military cargo (including Military Sealift Command Voyage charters). [Coordinate with Security Operations] • Is the Design Basis Threat (DBT) used when conducting VAs? • Are engineers a part of the vulnerability assessment team? (trained, established assessment guidelines) • Are engineering considerations, including local DBT and threat identified in the Threat Assessment, used when evaluating the effectiveness of existing countermeasures? • Have engineers performed a blast analysis of the structures identified as critical in order to develop protective measures? • Did the analysis take into consideration the DBT and the construction of the facility? • Did the analysis also include critical infrastructure?	DoD Std 6 DoD O-2000.12-H Chapters 7, 8, 9 Strategic Goal 1G
*SE-RM-04	**Risk Assessment.** A risk assessment shall be established and conducted annually as part of the risk management process. • Are engineers included in the selection, design, and construction of physical countermeasures identified to reduce the risk? • Have compensatory measures been identified for all risks that are accepted? • Has a plan of action been developed to implement the countermeasures? • Has the assessment been translated into action items for either resourcing or procedural corrections? • Have waivers been requested when risk is accepted (if required)?	DoD Std 3 JP 3-07.2 AP D-1 DoD O-2000.12-H, Chapter 8 Strategic Goal 1H FM 3-100.12
2. AT PLANNING		
*SE-PLN-01	**Engineering Support to the AT Program.** Engineering support shall be included in the AT Program and discussed in the AT Plan. • Does engineering support to the AT Program integrate HHQ guidance (DoD, COCOM, Service)? • Has an appropriate entity been tasked in the AT Plan to provide engineering support to the AT Program? • Are engineering tasks specifically spelled out in the AT Plan? • Are these tasks adequate to support the AT Program (i.e., barrier plan, repair of security aids, recovery actions)? • Is the engineering department able to execute these tasks?	DoD Std 7

	• Does the AT Plan establish coordination responsibilities between the AT staff and Engineers? • Does the AT Plan address coordination between the installation and tenant units to ensure AT Construction criteria, DBT mitigation, facility layout, barrier plans, standoff, and site evaluation/selection criteria established by the installation AT Plan are adhered to?	
*SE-PLN-02	The Installation Commander shall integrate barriers into all physical security systems. Barrier planning shall be included in the baseline posture as well as the FPCON system. **BASELINE BARRIER PLAN** • Has a barrier plan been developed at the installation, facility or ship level? • Does the baseline physical security system include interior barriers for critical assets identified in the Criticality Assessment? • Does the baseline barrier system (perimeter, ACP, and interior) support procedural security requirements? • Is the baseline barrier system based upon the DBT or other threat factors (criminal, FIS, etc.)? • Does the barrier system mitigate the identified threats? • Is the baseline barrier plan written to clarify who, what, when and where to assist in carrying out mitigation strategies including barrier placement, ACPs, and alternate parking? • Are tenants included in the baseline barrier plan? **FPCON BARRIER PLAN** • Has a barrier plan been developed to support the FPCON System? • Is the plan appropriately resourced (e.g., barriers, equipment)? • Is the FPCON barrier plan written to clarify who, what, when and where to assist in carrying out mitigation strategies including barrier placement, ACPs, and alternate parking? • Are tenants included in the FPCON barrier plan? • Are facilities that cannot be protected included in the curtailment plan? • Are there means for emergency procurement of barriers? **GENERAL** • Are barrier plans reviewed annually and refined as needed?	DoD Std 13 (Baseline), 22 (FPCON) JP 3-07.2 Chapter VI DoD O-2000.12-H, Chapters 7, 8, 9 Strategic Goal 2D
SE-PLN-03	Commanders shall establish an ATWG to implement the AT program, develop/refine the AT plan, and address emergent AT program issues. [coordinate with Security Operations Specialist] • Are engineers a part of the Antiterrorism Working Group (ATWG)?	DoD Std 10 DoD O-2000.12-H, Chapters 7, 8, 9 Strategic Goal 2A

SE-PLN-04	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. New construction and renovation projects for billeting, PGB, inhabited facilities should include an antiterrorism review at all stages of planning, programming, design, and construction. Review selected appropriate DD Forms (Form 1391) to ensure antiterrorism is adequately covered and supports the installation's plans. All projects regardless of funding must comply with the latest DoD Construction Standards. • Are the procedures established and identified in the AT Plan for AT construction standards? (Adopt or supplement UFC) • Does construction design include strategies to provide greater resistance to terrorist attack? o Maximize standoff distances? o Prevent of building collapse? o Minimize hazardous flying debris? o Effective building design layout? o Limit airborne contamination? o Mass notification? o Facilitates future upgrades? • Is there an identified waiver process? • Are planners, designers, engineers and security personnel aware of the latest DoD AT Standards, UFC, and COCOM criteria? • Is there a process in place to perform formal reviews of projects with the appropriate personnel? • Are renovations and new construction designed IAW DoD AT standards? • Are Combatant Commander AOR and/or country specific AT construction standards/guidance incorporated into the facility planning process? • Is there a line item indicating the added cost of AT measures?	DoD Std 17 DoD O-2000.12-H, Chapters 7, 8, 9, 24 Strategic Goal 2I UFC 4-010-01 & 4-010-02
SE-PLN-05	The Installation commander shall establish a prioritized list of AT factors for facility and site evaluation/selection criteria. This process is applicable to buildings occupied or under consideration for occupancy by DoD personnel. • Is a prioritized list of AT factors, including facility specific DBT, layout of the facility, barrier plan, standoff and construction, site evaluation/selection criteria, identified in the AT Plan? • Does the AT Plan identify who has authority to deviate from criteria and provide a process for requesting, justifying, and documenting documents deviations?	DoD Std 17 DoD O-2000.12-H, Chapters 7, 8, 9
	PHYSICAL SECURITY PROGRAM	
SE-PLN-06	The Installation Commander shall develop and implement threat risk mitigation measures to reduce the vulnerabilities of DoD critical assets to terrorist attack and integrate these measures into overall AT program efforts. [Coordinate with Security Operations] • Have hardening, retrofit or relocation measures been developed for identified critical facilities? • Are these measures based upon regulatory requirements or the result of a vulnerability assessment	DoD Std 7 DoD O-2000.12-H UFC 4-010-01 & 4-010-02

	• Have building protection measures been developed based upon the DBT?
	• Are risk mitigation measures for critical facilities included in the AT Plan as part of the Physical Security Program or the FPCON system?
	• Have AT technologies been incorporated into protective system designs in the following categories?
	  o Detecting and defeating improvised explosive devices
	  o Physical Security
	  o Protecting inhabited facilities such as billeting, PGS and MEVAS
	• Does the installation use technology to mitigate vulnerabilities where applicable?
	• Does the engineer, planner, or security personnel know where to look for technology assistance (e.g., PSEAG, TSWG, UFC and related DoD publications)?	

	STANDOFF	
	The most effective protection from a bomb blast is standoff. Standoff is the distance between an occupied 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.	
	PERIMETER STANDOFF	

*SE-PLN-07	Standoff distances between the installation's (controlled or uncontrolled) perimeter, and occupied buildings should be appropriate to the use, type of construction, population of the building.
	• Is perimeter controlled or uncontrolled? (Controlled perimeter requires physical measures that preclude vehicles from reasonable access; e.g., perimeter fence, woods, berms, ditches, farm fields without access roads, etc).
	• How is the controlled perimeter defined?
	  o What kind of protection system is used?
	  o Is it temporary or permanent protection?
	• Is the controlled perimeter able to stop the identified moving vehicle DBT?
	• Are perimeter standoff distances (controlled) IAW building occupancy, construction or population?
	  o Does the available distance between the controlled perimeter and the facility provide the level of protection required from the DBT?
	  o If not, have building hardening techniques been implemented to reduce the impact?
		DoD Std 17
		
		DoD O-2000.12-H Chapters 22, 23, 24
		
		Strategic Goal 2I
		
		UFC 4-010-01 & 4-010-02

	○ Have compensatory measures been implemented to protect facilities that do not have a controlled perimeter (i.e. facility barrier plans)? • Does the available distance between the compensatory measures and the facility provide the level of protection required from the DBT? • Is the use of facilities with insufficient standoff from a protected perimeter or facilities with that do not have a controlled perimeter curtailed during increased FPCONs? • Are there waivers for insufficient perimeter standoff? • Do off base housing facilities have the standoff required by the UFC or COCOM OPORD? ○ If not, are compensatory measures in place to reduce the effects of an attack? • Do expeditionary and temporary structures have the standoff required by the UFC or COCOM OPORD? ○ If not, are compensatory measures in place to reduce the effects of an attack?	
SE-PLN-8	Adjacent land use should be evaluated to determine the need for obscuration screening or additional measures necessary to preclude: • Can a direct line of sight be avoided by obscuration screening, planting trees, or other methods? • Are facility entrance doors positioned so they cannot be easily targeted from the installation perimeter or uncontrolled vantage points?	DoD Std 17 DoD O-2000.12-H, Chapters 22, 23, 24 UFC 4-010-01 & 4-010-02
	ACCESS CONTROL POINTS	
*SE-PLN-9	Access Control Points (ACPs). The overall layout, organization, infrastructure, and facilities of an ACP should be capable providing positive vehicle control and support access control procedures (vetting, inspection, rejection). ACPs should secure the installation from unauthorized access and the introduction of weapons / contraband while maximizing vehicular traffic flow and provide protection to personnel performing security functions at the ACP. • 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: ○ Are speed reduction devices used to slow incoming vehicles to, or below, the design speed of the ECF? ○ Is the capability to sort traffic by vehicle type into the proper lane before reaching the inspection area or checkpoint integrated into the ACP? ○ Is adequate stacking distance provided for vehicles waiting for entry? ○ Can security personnel identify potential threat vehicles, including those attempting entry through the outbound lanes of traffic? • The Access Control Zone is the main body of the ECF and includes guard facilities and traffic management equipment used by the security forces. Factors to consider include: ○ Are devices in place to allow security personnel to maintain positive control of vehicles when performing vehicle and personnel	DoD Std 17 DoD O-2000.12-H, Chapters 22, 23, 24 Strategic Goal 2I UFC 4-010-01 & 4-010-02 UFC 4-022-01 Control Points

identification?
  - 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, obscuration from surveillance, accommodate one or more vehicles requiring inspection, and include rejection capability.
  - Can the ACP support tandem processing to limit the number of vehicles stacked in the approach zone?
  - 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.
- The Response Zone is the area extending from the end of the Access Control Zone to the final denial barrier. Factors to consider include:
  - Does the response zone provide the time and space needed to allow security force personnel, including overwatch 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.
  - Are final denial barriers incorporated into the ACP?
- 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:
  - Does each ACP offer minimum standoff distance from billeting, MEVAs, critical facilities and primary gathering buildings IAW DoD requirements?
- Personnel protection must be integrated into the ACP design. Factors include:
  - Does each ACP have hardened guardhouse with bullet resistance doors, window frame and glazing IAW DoD and COCOM OPORD requirements?
  - Are devices in place to protect personnel from oncoming vehicles (bollards, high curbs, walls, or other barriers)?
- Other considerations include:
  - Are barriers appropriate considering climate and terrain?
  - Are barriers in compliance with DoD crash resistance requirements?
  - Is obscuration incorporated into ACP design to limit hostile surveillance?
  - Are there an appropriate number of ACPs for the quantity and type of traffic (employee, visitor and commercial)?
  - Are the ACPs sited appropriately considering demand for access to the installation, traffic origin and destination, capability of surrounding road networks, and security?
- Unmanned ACPs/gates:
  - Are unused ACPs secured to at least the same level as the adjoining fence?
  - Are devices in place to prevent surreptitious vehicle entry?
  - Are barriers used at unmanned ACPs / gates in compliance with DoD crash resistance requirements?
  - Are high speed vehicular approaches eliminated?

	FACILITY STANDOFF	
*SE-PLN-10	Standoff for inhabited buildings, troop billeting, PGB structures, MEVAs, including parking areas and vehicle access, should be appropriate to the use, type of construction, population of the building, and, at a minimum, meet the required level of protection for the category of building. • Has blast analysis been performed for facilities with less standoff than that required by DoD standards to determine minimum standoff distances to achieve the desired level of protection? • Is parking controlled and how? • Are standoff distances from roads adequate to achieve the level of protection required? • How is standoff enforced? • Do the FPCON measures include measures for achieving additional standoff? o Are barriers properly designed / installed to provide the required level of protection from the DBT? o Are there plans to restrict parking? • Are there waivers for facility standoff?	DoD Std 17 DoD O-2000.12-H Chapters 22, 23, 24 Strategic Goal 2I UFC 4-010-01 / 4-010-02
SE-PLN-11	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. • Are trash containers located away from buildings? • What is the standoff distance? • Are trash containers secured?	DoD Std 17 DoD O-2000.12-H, Chapters 22, 23, 24 UFC 4-010-01 & 4-010-02
SE-PLN-12	Critical facilities, troop billeting and primary gathering buildings should not be located near large non-DoD populations. • Has adequate standoff been established? • Is obscuration used to prevent surveillance? • Have buildings in this category been included in FPCON measures to establish additional standoff, curtailment requirements, etc?	DoD Std 17 DoD O-2000.12-H, Chapters 22, 23, 24 UFC 4-010-01 & 4-010-02
SE-PLN-13	Landscaping around critical facilities, troop billeting and primary gathering buildings should not provide concealed areas. • Does foliage obscure hidden packages (i.e. higher than 6")? • Is there a maintenance or service plan to control vegetation and shrubs? • Is landscaping considered during facility planning? [engineering and security review]	DoD Std 17 DoD O-2000.12-H, Chapters 22, 23, 24 UFC 4-010-01 & 4-010-02

SE-PLN-14	Inhabited facilities should not have parking beneath or on top of the buildings.
	• If parking is allowed on top of or under the building has the building been hardened resist blast?
	  o Is building designed to resist progressive collapse?
	  o Are physical controls to restrict parking to authorized personnel only adequate?
	• Does the FPCON barrier plan include measures to restrict vehicle access to the distance required to provide a low level of protection from the established DBT?
		DoD Std 17
		
		DoD O-2000.12-H, Chapters 22, 23, 24
		
		UFC 4-010-01 & 4-010-02

SE-PLN-15	Expeditionary and temporary structures: Billeting groups, rows of billets, and individual billets should be separated in accordance with DoD construction standards, with appropriate fragmentation protection and sufficient bunker construction and capacity. • Is there sufficient and appropriate fragmentation protection? • Is appropriate standoff maintained between structures to limit fragmentation damage? • Are there a sufficient number of bunkers? • Does bunker design and construction provide adequate protection?	DoD Std 17 DoD O-2000.12-H, Chapters 22, 23, 24 Strategic Goal 2I UFC 4-010-01 & 4-010-02
SE-PLN-16	Mail and supply handling areas should be sufficiently separated from inhabited structures and constructed IAW DoD criteria. • Is the mailroom located away from high occupancy buildings and critical infrastructure? • Does it meet DoD UFC criteria? • Have blast protection measures been integrated into the mailroom facility design?	DoD Std 17 DoD O-2000.12-H, Chapters 22, 23, 24 Strategic Goal 2I UFC 4-010-01 & 4-010-02
SE-PLN-17	For troop billeting, PGB and inhabited areas, drive-up or drop-off areas should be configured so access by vehicles can be stopped at higher FPCONs. • Do drive-up and drop-off areas have provisions for restricting access? o Are barriers adequate to prevent unauthorized entry? • Does the FPCON barrier plan eliminate drive-up and drop-off areas?	DoD Std 13, 17 DoD O-2000.12-H, Chapters 22, 23, 24 UFC 4-010-01 & 4-010-02

SE-PLN-18	For troop billeting and PGB, high-speed vehicular approaches should be eliminated. If high-speed approaches cannot be eliminated, mitigation measures should be included in the FPCON measures. • Are barriers sufficient to prevent high-speed vehicular approaches? • Are mitigation measures included in FPCONs? o Can high-speed vehicular approaches be rerouted? o Does the FPCON barrier plan eliminate high-speed approach?	DoD Std 7, 17 DoD O-2000.12-H, Chapters 22, 23, 24 UFC 4-010-01 & 4-010-02
	BUILDING CHARACTERISTICS	
	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 calculations and identify mitigation measures identified in other SE report areas.	
*SE-PLN-19	Typical construction used in inhabited facilities, mainly: billeting, primary gathering buildings (PGB), on the installation, noting glazing, exterior wall, frame, floor, and roof types on buildings, shall be identified. • What is the typical construction of building components? o Walls (reinforced or un-reinforced): CMU, metal studs with exterior façade of brick or stucco? o Frame, roof, columns, beams, floor slab etc. o Steel/concrete/wood/: beam size, columns, floor and roof deck, etc. o Glazing type: annealed, tempered and/or laminated ▪ Has Fragment Retention Film (FRF) been installed (10 mil minimum)? • Do windows reinforced with FRF have a catch bar? o Do windows have blast curtains? • Are exterior walls retrofitted to resist DBT? o What was the retrofit method?	DoD Std 17 DoD O-2000.12-H, Chapter 24 Strategic Goal 2I UFC 4-010-01 & 4-010-02
SE-PLN-20	For targets selected by the Terrorist Operations Specialist, data collected will include: general building information, construction details and drawings, adjacent area information, and vulnerability considerations. This data will be used to develop graphical representations of weapons effects. • What are the components of building? • Exterior and interior walls, frame, roof, columns, girders, beams, glazing etc. • Location from adjoining buildings, parking, roadways • General construction of all adjoining buildings within damage radius generated by weapons	DoD Std 6 DoD O-2000.12-H, Chapter 24 UFC 4-010-01 & 4-010-02

	• Barrier location and material	
	WEAPONS EFFECTS	
	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 to suggesting mitigation strategies, use of this data will raise awareness of weapons effects on people and structures.	
SE-PLN-21	Installation commanders shall ensure essential security and engineering personnel tasked with developing mitigation strategies and design review complete appropriate formal training and education. Documentation of training should be in accordance with the DoD Component's requirements. • Have the essential Security and Engineering personnel properly been trained in Security Engineering criteria IAW COCOM or Service requirements? • Did personnel attend a "Security Engineering Course" given by Army Corps of Engineers or equivalent course? • Do engineers / security have a training plan to ensure they maintain proficiency? • Are essential personnel aware of the latest technological developments in order to select appropriate and cost effective counter measures? • Are Engineers and Security 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?	DoD Std 23 DoD O-2000.12-H, Chapter 18 UFC 4-010-01 & 4-010-02
SE-PLN-22	The ability of the installation to self-assess weapons effects on its buildings based on DBT greatly enhances the ability to develop and implement countermeasure strategies. Using available computer programs such as VAPO, BEEM, AT Planner, WINDAS, and HAZL etc will generate graphical representations of weapons effects that will aid in this process. This is a recommended practice. • Does the installation have ability to model blast effects? • Are personnel trained in the use of the modeling tools? • Is blast modeling analyses incorporated into mitigation strategies?	DoD Std 20 DoD O-2000.12-H, Chapter 12 Strategic Goal 2I UFC 4-010-01 & 4-010-02
	ILLUSTRATIVE TARGETS	
SE-PLN-23	Prepare range-to-effect, weapons effects vulnerability radii, and iso-damage contours charts for illustrative targets selected by the Terrorist Operations (TO) Specialist. Weapons effects charts should utilize the type and size weapon and tactic identified by the TO in weapons effects calculations. Proposed mitigation measures, such as window hardening, facility upgrades and effective barrier plans should be included.	DoD Std 6 DoD O-2000.12-H, Chapters 20, 22, 23, 24 UFC 4-010-01 & 4-010-02
SE-PLN-24	3-D graphics, showing the effects of bomb attacks on buildings and people, shall be prepared to support Emergency Management consequence analysis. This data will be used to graphically illustrate response requirements and the	DoD Std 6

	effects that mitigation measures have on reducing damage and casualties.	DoD O-2000.12-H, Chapters 22, 23, 24 UFC 4-010-01 & 4-010-02
	REAL PROPERTY UPGRADES	
*SE-PLN-25	DoD AT Standards UFC 4-010-01 and UFC 4-01002 apply to all DoD components, to all DoD inhabited buildings: billeting, PGs and including DoD expeditionary and temporary structures. Real property upgrades should address the necessary building components: • Is progressive collapse mitigated in buildings with three or more stories? • Do renovations address main framing, walls, columns, floors and roof member? • Does renovation address glazing components? • Do renovations address relocation of parking, if necessary? • Do renovations addresses obscuration screening? • Do renovations provide protection against fragmentation and blast pressure?	DoD Std 17 DoD O-2000.12-H, Chapters 22, 23, 24 Strategic Goal 2I UFC 4-010-01 & 4-010-02
SE-PLN-26	For expeditionary and temporary structures: Shelters should provide protecting from direct and indirect fire weapons • Has a DBT for direct and indirect fire weapons been established? • Have an appropriate numbers of shelters been provided? • Are the shelters constructed to protect against established the DBT?	DoD Std 17 DoD O-2000.12-H, Chapters 22, 23, 24 UFC 4-010-01 & 4-010-02
	PLANNING AND NEW CONSTRUCTION	
	The cost impacts of incorporating antiterrorism principles into new construction and renovation projects are least in the earliest design phases. Installation planners should be familiar with the latest UFC 4-010-01 and UFC 4-010-02 standards and incorporate them into all DoD inhabited buildings: billeting, PGS and including DoD expeditionary and temporary structures IAW with new construction, MILCON construction, Host-Nations and other foreign Government construction regardless of funding. Refer to UFC-4-010-01 for all limitations and applicability.	

	TERRORIST INCIDENT RESPONSE (TIR) / TERRORIST CONSEQUENCE MANAGEMENT (TCM)	
SE-PLN-27	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] **TIR REQUIREMENTS:** • Are installation engineers' part of the Emergency Operations Center (EOC) staff? • Have their roles and responsibilities been identified in the EOC Plan? • Are as-built drawings (latest design / construction drawing / shop drawings etc.) for all facilities available for use during an emergency? • 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? **TCM REQUIREMENTS:** ▪ Are installation engineers tasked, trained, and equipped to provide structural analysis of damaged buildings during consequence management operations? ▪ Perform structural analysis of buildings for immediate use? ▪ Provide recommendations for the repair or demolition and renovation / rebuilding of damaged structures	DoD Std 17 , 20, 21 DoD O-2000.12-H, Chapters 11, 12 UFC 4-010-01 & 4-010-02
	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: establish boundary; isolate activity and discourage visitors; and impede 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. <u>FPCON Measure ALPHA 2.</u> 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). 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).	

*SE-PLN-PORT-01	Waterside physical security system should include barriers to establish a boundary, isolate activities, and impede passage by boat or swimmer. [coordinate with Security Operations]
	• Is there a barrier plan to complement waterside security?
	  o Is standoff provided IAW FPCON ALPHA 2 and BRAVO 4?
	  o What kinds of barriers are used?
	  o Do barriers prevent direct unchallenged access onto piers, wharves, or docks when ships are moored?
	• Are barriers placed far enough from the assets to provide adequate protection based upon the design basis threat?
	• Do selected barriers provide surface and subsurface protection?
	• Are barriers installed at the land/water interface or at the mean high-water mark?
	• Barrier systems for land access to waterside operations must conform to requirements identified in previous barrier planning and standoff benchmarks
		DoD Std 7
		
		DoD O-2000.12-H, Chapters 22, C22.14, AP 17
		
		UFC 4-010-01 & 4-010-02

SE-PLN-PORT-02	Effective exclusion zones (safety and security) should be contained in plans to establish 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]	DoD Std 7, 13 DoD O-2000.12-H, Chapter 22, C22.14, AP 17 UFC 4-010-01 & 4-010-02
SE-PLN-PORT-03	Where parking is necessary on piers, wharves, or docks, it shall be limited to essential government or vetted commercial vehicles. • 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? • Do parking locations provide standoff IAW DoD criteria?	DoD Std 13, 17 DoD O-2000.12-H, Chapter 22, C22.14, AP 17 UFC 4-010-01 & 4-010-02

	PHYSICAL SECURITY MEASURES FOR AIRFIELDS	
	Airfields 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; 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 Combatant Commander requirements for enhanced physical security protection for many types of munitions stored at DoD air fields	
SE-PLN-AF-01	The AT Plan shall include protection of airfields located on the installation. [Coordinate with Security Operations Specialist] • Does the plan address: o Barrier systems for access to the airfield that conform to requirements identified in previous barrier planning and standoff benchmarks o Airfield ACP design and construction that conforms to requirements in previous ACP design and construction benchmarks o Standoff considerations for airfield facilities, aircraft, equipment, and other assets that conform to previous perimeter and facility standoff benchmarks	DoD Std 7 UFC 4-010-01 & 4-010-02
SE-PLN-AF-02	The installation commander shall provide protection DoD assets located on installation airfields. [Coordinate with Security Operations Specialist] • Does airfield security include the following components? o Integrated defense in depth o Hardening of selected buildings against attack o Airfield specific FPCON measures o Are runway and taxiways included in the protection scheme, to include the utilities that may be buried beneath them? [Coordinate with Infrastructure Engineer] o Are aircraft parked within a restricted/controlled area? o Is there a separate airfield perimeter fence (requirement depends on type of resource and installation perimeter)? o Is positive access control provided for sensitive airfields (e.g., Priority Level resources, alert aircraft, and DV aircraft)? o Are barriers in place to control vehicle access? o Are high-speed approaches mitigated? o Are parking areas prominently marked with warning signs? o Is there a process to limit vehicle access points for increased threats?	DoD Std 13, 17 DoD O-2000.12-H, Chapter 22, C22.12, UFC 4-010-01 & 4-010-02

Annex D
Infrastructure Engineering Benchmarks

The installation's utilities infrastructure are 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 are 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, industrial and potable water uses. Communications systems support mission critical voice and data systems. Bulk fuel storage and refueling are 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	**Threat Assessment.** Installation Commanders shall establish a Threat Assessment 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. • Does the TA address all hazards for infrastructure supporting installation's mission? • Are threats to infrastructure and warnings disseminated to persons responsible for infrastructure protection?	DoD Std 4 JP 3-07.2, Ch. III, VI, & AP B DoD O-2000.12-H, Chapter 5 DoD O-2000.12-P, Strategic Goal 1E
IE-RM-02	**Criticality Assessment.** 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. • Does CA identify assets necessary for mission accomplishment to include supporting infrastructure? o Are single points of failure identified for the installation infrastructure? o Has the infrastructure critical to DoD, but not necessarily important to the installation, been identified? • Has the installation identified critical assets off the installation when there are no alternative or independent systems on the installation? • Does CA address effect of loss (local and strategic), recoverability, mission functionality, substitutability, reparability of installation assets and supporting infrastructure? • Does assessment address duration of operations issues? Food, water, shift	DoD Std 5 DoD O-2000.12-H, Chapter 6, 22 Strategic Goal 1F

	changes in CBRNE environment? • Does the impact of loss to include local and strategic missions? • Have mission essential/critical personnel been identified? (personnel responsible for operation and maintenance of critical infrastructure) o Is there a process for identification, recall, and response by critical personnel? [Coordinate with Security Operations] • Are offices responsible for infrastructure, e.g. PWD or CE, and the fire department, aware of the priority on assets? • Is there additional infrastructure that may not be directly tied to the installation but has an importance to DoD? • Report any infrastructure that is not on the CA to the Terrorist Operations specialist	

IE-RM-03	**Vulnerability Assessment.** Installation Commanders shall provide a terrorist 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.
	• 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]
	• Are Public Works/BCE engineers assigned to installation's VA team?
	  o Have the engineers been trained on how to conduct a VA?
	  o Is there specific methodology established for the assessment of infrastructure?
	• Are infrastructure vulnerabilities entered into the Core Vulnerability Assessment Management Program (CVAMP) and tracked until mitigated?
	• 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?
	• Does the assessment address all hazards: terrorism, fire, wind, equipment failure, etc.?
	
	WATER SYSTEM VULNERABILITY ASSESSMENT (WSVA)
	• Has installation conducted a WSVA covering the following areas:
	  o Water system serving 25 or more DoD consumers
	  o CONUS water systems serving over 3300 fall under EPA regulations.
	  o OCONUS water from local supplier needs WSVA
	  o Consecutive and unregulated system in CONUS needs WSVA
	• Does the Water VA cover the following areas?
	  o Review of pipes and conveyances
	  o Physical barriers
	  o Water collection, treatment, storage facilities
	  o Automated systems used by water system
	  o Use and handling of chemicals
	  o O&M of the system
	• What type water testing is being performed and at what intervals?
	• Can testing be varied according to threat?
		DoD Std 6
		
		DoD Memo 3 Jul 03 - Water Policy
		
		Strategic Goal 1G
		
		OPNAVINST 11300.6A 5500.14D
		
		NAVMC DIR 3500.86

IE-RM-04	**Risk Assessment.** A risk assessment process shall be established for the installation and reviewed annually, and should include critical infrastructure and assets. • Is the assessment used to justify physical security changes for protection of	DoD Std 3 JP 3-07.2, AP D1

	infrastructure (physical and cyber)? o Is the DBT used when developing protective measures? • Does the risk assessment provide Critical Asset assurance analysis, planning, prioritization, resource programming, and response necessary to mitigate the disruption or loss of critical assets? • Can critical functions be transferred to alternate locations and resume operations quickly, without an unacceptable degradation to the mission? • Have protective/compensatory measures for critical infrastructure been developed? o Have contingency plans been developed for the long term or temporary loss of the infrastructure? • Have plans been developed by the owner /user for protection of critical infrastructure/infrastructure critical to mission accomplishment? • Have high risk vulnerabilities been mitigated or their plans in place to mitigate these vulnerabilities? [Coordinate with Terrorist Operations] • Are engineers included in the selection, design, and construction of physical countermeasures identified to reduce the risk? • Have compensatory measures been identified for all risks that are accepted? • Has a plan of action been developed to implement the countermeasures? • Has the assessment been translated into action items for either resourcing or procedural corrections? • Have waivers been requested when risk is accepted (if required)?	DoD O-2000.12-H, Chapter 8 Strategic Goal 1H
IE-RM-05	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. • Is chief aware of primary gathering and mission essential buildings? • Does the chief accomplish a fire risk survey in accordance with service guidance? • Has a fire risk assessment study been determined for the installation, to include each building? • Are buildings rated according to risk? • 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?	DoD Std 21 DoDI 6055.6, Encl. 2, Par 1.b and c AR 420-90, Chapter 60 AFI 32-2001 OPNAVINST 3440.17
2. AT PLANNING		
2.A	**AT PLAN ELEMENTS**	
IE-PLN-01	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. • Is infrastructure addressed in the AT Program / Plan? • Are critical missions prioritized for utility support? • 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? • Resource support infrastructure function?	DoD Std 7 DoD O-2000.12-H, Chapter 9, AP4 Strategic Goal 2D

	• Public Works/BCE?	
IE-PLN-02	The Installation Commander shall develop and implement site-specific FPCON measures for the protection of infrastructure critical to mission accomplishment. • Was the threat assessment used to develop levels of protection for infrastructure? • Are measures in place to implement the following FPCON measures? o FPCON Measure BRAVO 2: Has the installation developed a plan to control access to critical infrastructure? o FPCON Measure BRAVO 3: Has buildings housing critical infrastructure been identified and provided protection against IED threats? o FPCON Measure BRAVO 4: Have rooms containing infrastructure systems been secured? o FPCON Measure BRAVO 8: Is there a process to conduct random inspections of water? o 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)? ▪ 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? o FPCON Measure CHARLIE 6: What is the plan to implement monitoring of chemical and biological agents? Is there a process to prevent unauthorized taps into facility water systems? o 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?	DoD Std 22 DoD O-2000.12-H, Chapter 10 Strategic Goal 2F
IE-PLN-03	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 a crisis situations. • Have services been identified which are so essential they must continue during a crisis situation? • Do plans address contractor access to base and critical facilities? • Do contingency plans require military members to replace contractor employees during a crisis or contingency?	DoD Std 18
2.B	**CRITICAL INFRASTRUCTURE SINGLE POINTS OF FAILURE (SPF)**	
IE-PLN-04	Critical infrastructure support elements should not be co-located to prevent or minimize multiple support systems from being destroyed simultaneously. • Are Critical systems and nodes co-located? • Are facilities and habitat areas adequately separated from overhead high-voltage lines? • 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?	DoD Std 19

IE-PLN-05	Utility distribution systems on the installation should be arranged in a looped configuration. In the absence of a looped system, a redundant or physically diverse system, or alternate system should be available. • Are water distribution systems looped to prevent dead ends in system? • How many telephone switches serve the installation? • Are remote switches capable of independently handling telephonic traffic in case of an outage at the dial control office? Identify those key distribution system components susceptible to damaging wind effects up to normal area maximums • (i.e., Component name, identification, wind speed, and/or duration limitations). • 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? • Are key distribution system components protected from electrical surge or lightning strike? • Are key distribution system components protected from rain, water, or flooding effects? • Are key distribution system components protected from heat and humidity (not fire) effects? • Are key distribution system components resistant to cold and icing effects? • Are key distribution system components protected from hail damage?	DoD Std 19
2.C	**COMMUNICATIONS**	
IE-PLN-06	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. • Are the systems protected with passwords and firewalls, including modems and RF access? • Does the site maintain a plan that addresses continuous availability of communications systems supporting missions (i.e., COOP? • 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)? • Do these plans address issues of redundancy, survivability, reliability, and security? • Does the plan address issues of prioritization, system restoration, communications systems usage, and emergency operations and • maintenance? • Have prioritization procedures been exercised to ensure that communications critical to executing EACH mission are not interrupted?	DoD Std 20

IE-PLN-07	The commercial communications cable route diagrams and interfaces affecting the installation are available to provide information for security, redundancy and diversity. • Are cable diagrams, paths/routes as described in the documentation, drawings, and diagrams?	DoD Std 19 Strategic Goal 3C
IE-PLN-08	Redundancy and diversity in communication systems should exist to avoid single point vulnerabilities. • Is there diversity in the media used (e.g. RF, SATCOM, fiber optic cable, copper cable and laser)? • What systems are available? • Which systems are used the most? • What networks support the systems (e.g. NIPRNET, SIPRNET, JWICS, DRSN)? • For activity cabling: • Is there diversity in the external routing? • How many cable entry/exist points onto the installation • 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? • If so, is there adequate separation in fibers or are they all in the same cable trench conduit or follow the same path? • What is the separation distance? • Is it sufficient to prevent a "backhoe" type incident? • Is it sufficient to keep the cables from crossing on the same bridge? • Is there physical diversity in the internal cable plant? • How many cable entry/exit points into the facilities? • Is there sufficient separation such to prevent a single event form severing both cable path connectivity? • 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 closests are side-by-side, where fire or other events in one will impact the other? • Are classified communications distributed in a Protected Distribution System (PDS)? Is PDS integrity maintained? • Is there more than one data processing, switching, routing or distribution facility? If only one, what is the impact of its loss? • What is the security, fire protection and utility requirements of communication facilities (work with other team members for this expertise)? • Are clean fire suppression systems used in communications and data processing facilities? • Is access to the communication facilities controlled and monitored? • 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/exists onto the installation. Even if multiple providers are not used/available, diverse, physically separated entry/exists onto the installation are required with	DoD Std 19 Strategic Goal 3C and 5E

	connectivity to multiple, physically separated central offices)?	
IE-PLN-09	Dependencies on and support provided to other infrastructure and critical assets and/or the communications systems should be identified. • Are roads and/or bridges on or near your site used as corridors for communications transmission media; i.e., fiber optic or copper? • Do all mission-critical communications elements that rely on electric power have dedicated emergency generators? • Do 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? • Are the emergency generators auto-start? • What are the emergency generators' fuel capacities (provide generator)? What is the fuel storage capacity? • Who is responsible for the maintenance of the HVAC systems (provide POC and name of organization)? • For HVAC systems that have been identified, is there a dependency on water? • Is the HVAC system used for mission essential equipment on backup power?	
IE-PLN-10	Computer controlled (DDC, DCS, or SCADA) utilities and mechanical systems shall be protected from unauthorized access by appropriate security measures. • Are the systems protected with passwords and firewalls, including modems and RF access? • Is the modem disconnected/turned off when not being utilized by authorized users? • Is DCC coordinated with shutdowns for SIP? • 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)? • Are passwords restricted to authorized users on a need to have basis? • On what platform does this monitoring and control system operate? • What organization (address and contact number) designed, installed, and operates this monitoring and control system? • Does the site have onsite or offsite operational and/or maintenance personnel for the monitoring and/or control system? How many? • How often are this system's operational parameters checked or monitored? • Does the site maintain replacement components for this monitoring and control system, or have appropriate contracts to ensure immediate response and repair?	DoD Std 19 TSWG SCADA Ver 1.0
2.D	**POWER**	
IE-PLN-11	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. • What is the source of electrical power? • Are all hazards included in the evaluation of power reliability, such as natural disasters including snow, ice, tornadoes, winds, floods, trees and vegetation, etc.? • Is the power capacity adequate for installation demand level?	DoD Std 19

	• Are there redundant electrical feeds to the installation? • Are electrical feeds physically diverse? • Are the electrical distribution lines in a radial or looped pattern? • Are there switches to route the electric around a disruption or fault? • Who maintains the power distribution lines? • Is there a plan for load shedding? • Are substation cross connects have sufficient capacity for required loads, or is a load study planned? • Are power outages recorded in a log for reference and history? • Are there frequent power outages? If so, what are the causes of outages? • How easily or quickly can power be restored? • Are there any spare transformers and other equipment?	

IE-PLN-12	The installation should provide backup generators at critical facilities, with enough capacity to support those facilities during prolonged periods of time (i.e. command and control centers, security desk, communication facilities, hospitals, fire department, etc). Backup power units should be maintained and tested on a regular basis.
	• Has a determination been made of what mission functions (what percentage) are not functional under generator power?
	• Are generators located at mission critical, facilities and life safety locations?
	• Are portable generators available for emergencies?
	  o Where are they stored?
	  o At what facilities can they be used?
	  o Are the number and capacity of them adequate?
	• Are generators regularly maintained and tested?
	  o Under actual load, load bank or no load conditions?
	  o Does load bank have inductive load?
	  o What is frequency of testing?
	• Do generators have an automatic transfer switch?
	• Are generators co-located with other essential equipment?
	• If not, who will start generators and how long will this take?
	• Is there a generator refueling matrix? Does it match the prioritization of mission-essential facilities?
	• Are fuel tanks for backup generators secured? Are tanks of sufficient size to support an extended outage?
	• What level of security is provided (s)? Fenced? DoD approved padlocked gate? Barbed wire? Lighted? Bollards?
	• Are tanks locked or placed inside a locked facility to prevent contamination and potential ignition?
	• If above ground, are tanks double walled and/or have spill containment (dike) that will prevent a running fire?
		DoD Std 19
		AFI 32-1063

IE-PLN-13	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.
	• Does the power contingency plan address elements such as:
	  o Description of system, locations
	  o Mission priorities
	  o Single line diagram
		DoD Std 20
		AFI 10-24
		AFI 10-211

	○ Essential personnel, names, phone # ○ Generators installed, locations, size, fuel capacity ○ Portable generators, pre-designated, ○ Uninterruptible Power Supply - UPS ○ Automatic Transfer Switch – ATS	
IE-PLN-14	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. • Where are critical nodes in the system? • 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? • Are facilities housing these activities vulnerable to attack by virtue of their location or quality of their construction?	DoD Std 19
IE-PLN-15	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. • Is there sufficient back-up power (UPS) to support required equipment in case of a primary power outage? • Is a UPS providing continuous backup power during power interruptions? • Are batteries under maintenance? • Is the UPS room kept at temperature storage requirements for batteries? (77˚F optimal for gel cell) • Are battery rooms ventilated and/or alarmed?	DoD Std 19
IE-PLN-16	Access Control Points / Entry Control Points should have backup power for electronic equipment, and controlled vehicle barriers to sustain an extended primary power outage. Computers should also have a UPS in addition to backup power. [Coordinate with Security Operations] • Is there a backup power system for the ACP? • Is lighting within 100’ of the ACP also on this backup power? • Do computer processors used for screening or security also have a UPS?	DoD Std 19 UFC 4-022-01
2.E	**WATER DISTRIBUTION AND SUPPLY**	
IE-PLN-17	Water systems should have the capability to meet current water needs of critical assets (capacity, redundancy, reliability, etc.) • What type of contract does the site have with the water distribution provider? • Does the site have an emergency provisions contract with the provider? • Where are the points of connection to the external water system and flow capacity? • What is the site’s average water usage (gallons per day) (summer and winter, if significantly different)? • How much water is required for critical mission accomplishment (gallons per day) (summer and winter, if significantly different)? • Does the water system meet supply demands of potable, industrial, and fire-fighting water to support the critical mission?	DoD Std 7

	• Does the site's backup capability provide an adequate supply of potable, industrial, and fire-fighting water to support the critical mission? • How long (hours or days) will the site's storage capability sustain the demands for water during critical mission accomplishment? • What is the operating pressure range of the network? • How is the water pressure maintained? • Does the site have backup or auxiliary pumps to maintain network pressure? • Does the site have backflow prevention devices? • Has the site experienced disruptions to water service, or have any significant events occurred in the past that affected water service? • Are there sufficient onsite personnel to operate the water system during crisis or high demand, to include essential personnel designated to enter the site (i.e., natural disaster, heightened threat, or system disruption)? • What chemical treatments (chemical types) are used in providing water to the site, and where are they stored? • Does the system share rights-of-ways with other infrastructures? **SECURITY** (Coordinate with Security Operations) • Are treatment plants locked and secured to prevent unauthorized access? • Is the treatment plant staffed 24/7? • Do treatment plants have the necessary lighting, cameras, intrusion detection systems, or alarms to provide adequate monitoring?	
IE-PLN-18	Documents will be maintained detailing the current configuration of the water distribution system supporting critical assets. • Does the site maintain current drawings, blueprints, maps, schematics, timetables, line drawings, and photographs of potable water system key assets? • Are Geographical Information System (GIS) or Computer-aided Design (CAD) formats available? • What date was the last revision of the items identified • Has this information been protected, not been made available to the public, and kept in a secure onsite location?	DoD Std 19
IE-PLN-19	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. • Does the water contingency plan address elements such as: o Site maps, cutoff valves o Essential personnel, names, phone # o Spare parts o POC for water containers, bottled water, vendors o Water curtailment plan, priority o Plan for public notices o Fire dept. alternate source	DoD Std 21 DoD Memo 3 Jul 03 Water Policy AFI 10-21 AFI 10-211

2.F	FIRE PROTECTION	
IE-PLN-20	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. • Is there a central fire communications center? • Is the fire communications center adequately equipped with appropriate fire alarm monitoring, communication, and recording devices? • Are the alarms transmitted by radio or over copper/fiber lines? • Do the lines pass through a single point of failure?	DoD Std 20
IE-PLN-21	Equipment in mission critical facilities should have fire protection to protect equipment critical nodes and minimize damage. These facilities may include telephone switch rooms, NIPRNet and SIPRNet hubs, satellite links, and alarm panels. • Is a clean agent suppression system use as a first response to fire? • Handheld fire suppression equipment? Adequate in respect to location and type?	DoD Std 21 AF ETL 02-15
IE-PLN-22	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. • What are the fire evacuation plans/escapes routes, emergency lighting, and exits? • Does the installation have a written fire prevention plan? • What are the fire training, drills, and fire awareness programs? • Is there sufficient number of fire inspectors? • Is the fire department included in the design review process? • Are life-safety systems (panic hardware, exit lights, emergency lights, fire extinguishers, and stairs) installed and functioning? • Are existing buildings, new construction and major renovation projects in compliance with life safety code requirements? • Are fire-protection systems (sprinkler or suppression systems) installed and maintained in buildings according to the fire-safety codes? • Are fire hydrants inspected and maintained adequately? Who performs these functions? • Do fire hydrants have backflow preventers or fire department locks? • Are fire-alarm systems installed and maintained in buildings according to NFPA fire-safety codes? • Do fire detection and suppression systems transmit an alarm to the fire communications center? • What is the heat/smoke detection and alarm capability? • How is it maintained, tested? • What are the building smoke-evacuation capabilities?	DoD Std 21 DoDI 6055.6 NFPA 101 UFC 3-600-01

2.G	**BULK FUEL**	
IE-PLN-23	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. • Is fuel storage area easily accessible by fire equipment? • Is storage area adequately separated from primary gathering buildings and mission critical buildings? • Can fuel be supplied from bulk storage during power failures?	DoD Std 19
IE-PLN-24	The fuel system should meet the identified needs of critical assets. • List the consumption and storage (days of supply) requirements (by type). • What types of petroleum products and their quantities are available at the site? • Who are the fuel distributors serving the site? (Identify company name, company address, and types of fuel provided) • Who are the fuel distributors' points of contact (POCs)? (office name, and telephone numbers) • What is 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.) • How is the fuel delivered to the site (i.e., pipeline, tanker, barge, tanker truck, or railcar)? • 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.)	DoD Std 19
IE-STD-25	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. • Does the fuel contingency plan address elements such as: o Description of system, locations o Mission priorities o Refueling matrix? o Essential personnel, names, phone # o Generators installed, locations, size, fuel capacity o Agreements with alternate fuel suppliers?	DoD Std 20
IE-PLN-26	The location of the fuels 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. • Where are critical nodes in the system? • Is there positive control of fuel delivery and storage on the installation? • 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? • Are facilities housing these activities vulnerable to attack by virtue of their location or quality of their construction? • Can berms around storage tanks contain 110% of fuel tank storage?	DoD Std 19

IE-PLN-27	Oxygen storage containers should have appropriate standoff from buildings and flammable material. • Is the container protected from weather if not designed for external placement?	DoD Std 19 DoD 6055.9 NASA NSS 1740.15
2.H	**CBRN**	
IE-PLN-28	Installation personnel should review all new construction and major renovation projects to ensure Chemical, Biological, Radiological, and Nuclear (CBRN) protective measures are addressed. • Are CBRN protective measures addressed in the review of new construction and major renovation projects? (especially in regard to HVAC make-up air intakes and mailrooms) • Are new construction and major renovations designed to accommodate future addition of CBRN protective measures if not presently justified?	DoD Std 17 DoDI 2000.18 Strategic Goal 4E UFC 4-024-01
IE-PLN-29	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. • 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? • Are all vents, e.g. kitchen, bathroom, shut off during HVAC shutdown? • Is the plan incorporated into a mass notification plan? (See EM benchmarks) • Are CBRN detectors in operation? If so, what individuals are trained to operate the equipment? What is the CBRN detection architecture?	DoD Std 21 Strategic Goal 4E UFC 4-010-01, Standard 18
IE-PLN-30	. The need to establish collective protection for critical and essential personnel, 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. • Are 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. o Are CBR threats considered for mission critical facilities? • Is the level of protection based on CBR threat? • Would any attempt to interrupt or contaminate the HVAC delivery be detected by the site? • Have HVAC system operators and maintenance personnel practiced or exercised operations in CBRN environments within the past 12 months? • Are toxic industrial chemicals transported (by road or rail, etc) near the installation? • Can the HVAC system supporting a critical mission or asset operate independently if this monitoring and / or control system is not operational? • 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)?	DoD Std 21 UFC 4-024-01 FEMA 452 AFI 10-211

IE-PLN-31	Outside air intakes for HVAC systems, especially ones servicing mission critical rooms and facilities or primary gathering facilities, should be located at or above 3 meters (10 ft) from ground level or be provided with appropriate physical security measures to prevent the introduction of airborne contaminants. Height rule required for primary gathering facilities designed/constructed after FY2002. • Is the HVAC system of each building susceptible to attack? • Does the HVAC system have some type of fresh-air supply? • What is the ease of access to HVAC equipment? • Is it below ground with exterior airshaft? Is it at ground level? • Is it in a first floor mechanical room? If so, is the door kept locked? • Is it on the ground on the exterior of building? • Is it located at the second floor or higher through wall or on roof? If so, is there an exterior ladder to roof? Is the ladder blocked to prevent unauthorized access?	DoD Std 17 UFC 4-010-01, B-4.1
IE-PLN-32	Chlorine gas containers, such as those used at water treatment facilities, 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. • Is chlorine gas stored in vicinity of primary gathering or mission essential buildings?	DoD Std 21
3. RESOURCE APPLICATION		
IE-RA-01	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. • Is all critical infrastructure vulnerability assessment data included in CVAMP (HHQ and local)? • Are critical infrastructure vulnerabilities tracked until mitigated? • Have unfunded requirements been identified to mitigate infrastructure vulnerabilities? • 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]	DoD Std 30 Strategic Goal 4D

Annex E
Emergency Management Benchmarks

1. AT RISK MANAGEMENT		
EM-RM-01	**Threat Assessment.** Installation commanders shall establish a Terrorism Threat Assessment (TA) process consistent with the principles outlined in DoD O-2000.12-H to identify the full range of known or estimated terrorist threat capabilities (including the use or threat of use of chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) and weapons of mass destruction (WMD) for those DoD elements and personnel that have antiterrorism (AT) responsibilities. These assessments shall be updated on an annual basis, or more frequently as the terrorist threat environment dictates. Assessments shall be tailored to local conditions and address terrorist groups' operational capability, intentions, and activity, and whether the operational environment is conducive to terrorist activity. • Does the local Threat Assessment (TA) address the potential threat of terrorist use of CBRNE weapons? • Does the local TA incorporate the Combatant Commands (COCOM) WMD/CBRNE TA? • Does the local TA identify the specific hazard ID, quantity, and location of toxic industrial chemicals/toxic industrial materials (TIC/TIM) located on and near the installation? - Identify stationary facilities and transportation modes having the potential of releasing TIC/TIMs (intentionally) that could impact the installation. Some areas to consider are chemical facilities; refineries; railroads; highways; petroleum, oil, and liquid (POL) tanks farms; nuclear power plants, etc. • Has the installation contacted the Local Emergency Planning Committee (LEPC) to identify TIC/TIMs that could potentially affect the installation from the surrounding community? [link to locate all LEPCs: http://yosemite.epa.gov/oswer/lepcdb.nsf/HomePage?openForm]	DoD Std 4 E3.4.1. DoDI 2000.18, Guideline 8 DoD O-2000.12-P, Strategic Goal 1E
EM-RM-02	**Criticality Assessment.** Installation commanders shall establish a Criticality Assessment (CA) process consistent with the principles outlined in DoD O-2000.12-H and consistent with DoD Standard 3 to identify, classify, and prioritize mission-essential assets, resources, and personnel critical to mission success. CAs shall also be conducted for non-mission essential assets such as high-population facilities, mass gathering activities, and any other facility, equipment, service, or resource deemed important by the commander warranting protective measures to ensure continued efficient operation; protection from disruption, degradation, or destruction; and timely restoration. • Has the installation identified mission-essential assets, resources, facilities, or mission-essential vulnerable areas (MEVA) required for accomplishing terrorist incident response and terrorist consequence management measures i.e., emergency operations center, fire department, hospital, etc?	DoD Std 5 E3.5.1. DoDI 2000.18, Guideline 8 Strategic Goal 1F

EM-RM-03	**Vulnerability Assessment.** Installation commanders shall establish a Terrorism Vulnerability Assessment (VA) process consistent with the principles outlined in DoD O-2000.12-H and the DoD Drinking Water Policy to provide a vulnerability-based analysis of mission-essential assets, resources, and personnel critical to mission success that are susceptible to terrorist attack. **CBRNE VULNERABILITY ASSESSMENT (VA)** • Has an annual local CBRNE VA been conducted and documented by the installation? [can be a subsection to the local VA] • Is the local CBRNE VA based on threats identified in the local TA? • Is the local CBRNE VA conducted IAW DoDI 2000.18, Guideline 1 and 8? • Does the AT Plan contain guidance for conducting a local CBRNE VA? • Was the local CBRNE VA conducted and documented using the CBRNE VA Template? [template developed by DTRA and approved for use DoD-wide by the Joint Staff, J-34. Available on the ATEP or can be requested through DTRA at ATFPHelp@dtra.mil] • Does the local CBRNE VA address the following at a minimum? o CBRNE Emergency Response Plan o Mass Casualty Plan o Defense Continuity Plan [Continuity of Operations Plan (COOP)] o Terrorist Incident Response and Terrorist Consequence Management measures o Emergency operations center o First and emergency responder capabilities for installation/local (fire, hazmat, security forces, medical, explosive ordnance disposal o CBRNE training for emergency responders o Personal protective equipment (PPE) o Mass decontamination procedures and equipment o CBRNE detection equipment o Mass notification systems o Facility design and construction (HVAC systems, collective protection) o Evacuation and shelter-in-place procedures o AT Exercises and Training Program o Sustainment operations and follow on support o Memorandum of Understanding/Agreement (MOU/MOA)	DoD Std 6 E3.6.1.1. DoDI 2000.18, Guideline 1 & 8 DoD O-2000.12-H, Ch. 11 Strategic Goal 1G
EM-RM-04	**FOOD VA** • Has a food security program been established by the installation commander? • Has an office of primary responsibility (OPR) been identified for the installation? • Has a multi-disciplinary Food Security Assessment Team (FSAT) been established to conduct systematic review and assessment of the installation food systems? • Has an annual Food VA been conducted IAW applicable COCOM or Service AT guidance? o Does the Food VA identify potential vulnerabilities for each retail and military eating establishments such as dining facilities; AAFES / NEX / MCX facilities; Morale, Welfare, and Recreation facilities; etc? o Does the Food VA follow guidance in TG 188, *US Army Food and Water Vulnerability Assessment Guide*, AFI 10-246, *Food and Water Protection Program*, or other COCOM or Service guidance?	DoD Std 6 Applicable COCOM AT Guidance

	○ Has the installation developed written procedures for implementing the following Force Protection Condition (FPCON) Measures? ○ Measure ALPHA 5: Initiate food and water operational risk management procedures, brief personnel on food and water security procedures, and report any unusual activities ○ 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 ○ 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 ○ 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	
2. AT PLANNING		
	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.	DoD Std 15 E3.15.1.
EM-PLN-01	**AT MEASURES FOR OFF-INSTALLATION FACILITIES, HOUSING, AND ACTIVITIES** • Has emergency notification procedures for alerting off-installation facilities, housing areas, primary gathering building (50 or more DoD personnel), etc. of a terrorist incident been developed? • Do procedures identify who, what, when, where, and how personnel conduct evacuations or shelter-in-place procedures? • Are these procedures addressed in the AT Plan? • Are personnel trained to conduct these procedures and have they been exercised?	DoD Std 15 DoDI 2000.18, Guideline 1 Strategic Goal 2G
	Risk mitigation measures. Installation commanders shall develop and implement risk mitigation measures to reduce the vulnerabilities of DoD critical assets to terrorist attack, with emphasize on risk management, and integrate these measures into overall AT program efforts. Critical assets include those assets designated as Defense Critical Infrastructure per UFC 4-021-01 and distributive information and computer-based systems and networks. Include coordination with the appropriate local, State, Federal, or host-nation authorities responsible for the security of non-DoD assets deemed essential to the functioning of DoD critical assets and overall capability of the DoD to execute the National Military Strategy.	DoD Std 19 E3.19.1.

EM-PLN-02	**CRITICAL ASSETS** • Has the installation identified those critical assets that are vital to the successful accomplishment of the installation's mission following a terrorist incident i.e., emergency operations center, fire department, hospital, etc.? • Do these critical assets qualify as Mission Essential Functions (MEF) IAW DoDI 3020.26, *Defense Continuity Program* (DCP)? o If designated a MEF, is it included in the installation DCP Plan [see EM-PLN-04 for further questions] • Are evacuation and shelter-in-place (SIP) procedures developed if the critical asset is a facility? o Do SIP checklists provide adequate guidance to facility occupants i.e., shutdown HVAC system, exhaust fans; close/tape windows, doors; relocate to higher floors or interior windowless room, etc.? o Are supplies available to conduct SIP? (Tape, plastic, towels, etc.) • Are protective masks provided to personnel who may be required to SIP due to critical mission requirements of the facility? [See DoDI 2000.16, Std 21, for requirements] o Are personnel trained to use protective masks? o How is the shelf-life for protective mask filters tracked? • How is mass notification conducted for facility occupants? o Are procedures developed and exercised? • Do emergency response vehicles have adequate access to the facility? • Are procedures established to permit access for emergency responders during FPCON CHARLIE and DELTA?	DoD Std 19 DoD O-2000.12-H, C1.4.1.15. DoDI 3020.26, E1.1.10. UFC-4-021-01
EM-PLN-03	**INFORMATION OPERATIONS CONDITION (INFOCON)** • Has an INFOCON program been implemented by the activity commander? • Has the activity migrated to the new INFOCON program using the DEFCON scale (note: CDRUSSTRATCOM directed by 27 Apr 06)? • Is the program based entirely on higher command direction or does the activity have supplemental local procedures? • Is Tailored Readiness Options (TRO) for specific incidents included in these procedures (e.g. virus/worm incident)? • Do local levels always remain at least as high as the DoD level? • Is there an effective training and certification program for INFOCON to ensure the activity can meet internal and external requirements (e.g. global exercises)? • Does the commander periodically raise the INFOCON levels to ensure INFOCON implementers (system and network managers) are trained and procedures tested? • Does the commander establish exit criteria when INFOCON levels are raised? o 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)?	DoD Std 19 Strategic Command Directive 527-1

EM-PLN-04	**Defense Continuity Program.** Installation commanders shall have a comprehensive and effective Defense Continuity Program (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 shall validate, update, and reissue plans every 2 years, or more frequently as changes warrant. • Has a Defense Continuity Program (DCP) and Plan been developed? [Continuity of Operations (COOP) for some Services] • Has the installation identified and prioritized its organizational Mission Essential Functions (MEF)? [a MEF is the specified or implied tasks required to be peformed 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 ability to provide vital services, or exercise authority, direction, and control.] • Does the DCP Plan: o Provide guidance to continue MEFs within 12 hours and be capable of sustaining MEFs for up to 30 days? o 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? o Identify relocation sites or platforms for component use during continuity threats or events. Site selection should consider geographical dispersion, and maximum co-location and dual-use facilities? o Provide for identification, storage, protection, and availability for use at relocation sites, the vital records, material, and databases required to execute MEF? o 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? o Ensure that continuity programs are adequately planned, programmed, and budgeted, and that DCP-unique requirements are specifically identified in their budgets? o 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? o Has the DCP or COOP Plan been tested and exercised at least annually or as otherwise directed, to evaluate readiness?	DoD Std 19 DoDD 3020.26 DoDI 3020.42 Federal Preparedness Circular 65

	Terrorist Incident Response Measures. Installation commanders shall develop Terrorist Incident Response measures consistent with the principles outlined in DoD O-2000.12-H and include these measures in the overall AT plan. These measures shall include procedures for determining the nature and scope of incident response (including incidents with a CBRNE component); procedures for coordinating security, fire, medical, hazardous materiel, and other emergency responder capabilities; and steps to recover from the incident while continuing essential operations.	DoD Std 20 E3.20.1.
EM-PLN-05	**TERRORIST INCIDENT RESPONSE (TIR) MEASURES** • Has the installation developed TIR measures and included them in the AT Plan or referenced their location? • Do these measures include procedures for determining nature and scope of incident response; procedures for coordinating security, fire, medical, and explosive ordnance disposal emergency responders, etc? o Do procedures address bomb threats, hostage situations, anti-hijacking, assassinations, vehicle-borne improvised explosive devises (VBIED), etc.? o 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.)	DoD Std 20 DoDI 2000.18, Guideline 3 Strategic Goal 2D
EM-PLN-06	**NATIONAL RESPONSE PLAN (NRP) AND NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS) IMPLEMENTATION** • Has the installation adopted and implemented NRP policies and guidance? o Has Emergency Support Functions (ESF) been developed as described in the NRP? [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. There are 15 ESFs in the NRP] o Are OPRs (office of primary responsibility) assigned to each ESF? • Has procedures been implemented consistent with the NIMS and the Incident Command System (ICS) at all DoD domestic installations IAW the DEPSECDEF Memo "Implementation of the National Response Plan and National Incident Management System," dated 29 Nov 2005? • Has the installation commander's staff, EOC staff, and emergency responder's completed the following Federal Emergency Management Agency independent study courses as required by the above memo? o IS-100 Introduction to Incident Command System (ICS) o IS-200 ICS For Single Resources and Initial Action Incidents o IS-700 National Incident Management System (NIMS), An Introduction o IS-800.A National Response Plan (NRP), An Introduction o Note: There are several additional IS-100 courses available for healthcare/hospitals, law enforcement, public works, and schools o Are procedures established by the installation 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]	DoD Std 20 HSPD-5 NRP NIMS DEP SECDEF MEMO DoDD 3025.1

EM-PLN-07	**EMERGENCY OPERATIONS CENTER (EOC)**
	• Does the installation have a primary and alternate EOC?
	• Is the EOC operational 24/7 or activated when the situation dictates?
	  o Can the EOC be activated quickly and staffed if not manned 24/7?
	• Is the EOC Plan referenced or contained in the AT Plan?
	• Does the EOC Plan address:
	  o Activation, layout, and setup procedures?
	  o Recall procedures?
	  o Emergency notification rosters of appropriate agencies?
	  o Staff duties and responsibilities?
	  o Higher headquarters (HHQ) reporting procedures?
	  o BLUE DART reporting procedures?
	  o Communication capabilities and procedures?
	  o Resource dispatch and tracking?
	  o Compatibility / interoperability with local community emergency responders
	  o Equipment, supplies, and sustainability requirements for the primary and alternate EOC?
	  o Relocation / evacuation procedures?
	  o Security procedures (entry authorizations list)?
	  o Coordination considerations with local community / other agencies?
	• Are the following plans / checklists / standard operating procedures (SOP) maintained in the EOC?
	  o AT Plan
	  o Defense Continuity Program Plan
	  o Mass Casualty Plan
	  o CBRNE Emergency Response Plan
	  o Bomb Threat Plan
	  o Evacuation/Shelter-in-Place Plan
	  o Barrier Plan
	  o Infrastructure Contingency Response Plans (water, electrical, sewage, etc.)
	  o Suspected Aircraft Theft / Anti-hijack Plan
	  o Hostage Situation Plan
	  o Civil Disturbance / Riot Control Plan
	  o COCOM AT Operations Order
	• Does the EOC maintain adequate communications?
	  o Secure and non-secure telephones
	  o Secret Internet Protocol Router Network (SIPRNet) and Non-secure Internet Protocol Router Network (NIPRNet)
	  o Radio base station and or land-mobile radios
	  o Compatibility / interoperability with installation and local emergency responders
	  o Secure and non-secure fax
	  o Operational control of the mass notification system
	  o Television (commander's access channel, news, etc.)
	• Has C2 lines of communication been established with local / state EOCs?
	• Are installation grid maps posted, current, and acurate?
	  o Is the same scale grid map used by all emergency responder's?
	• Are activation and evacuation exercises conducted by EOC personnel?
		DoD Std 20
		
		DoDI 2000.18, Guideline 3
		
		Strategic Goal 2D

	• Are procedures established for monitoring incident development? • Are procedures established to request WMD Civil Support Team (CST) assistance?	
EM-PLN-08	**FIRE DEPARTMENT (FD) TERRORIST INCIDENT RESPONSE (TIR) MEASURES** • Does FD SOPs for CBRNE / hazardous material (HAZMAT) response address: o Establishing command, control, and communications (C3) consistent with the National Incident Management Systems (NIMS) and Incident Command System (ICS)? o Personnel accountability? o Fire suppression and search and rescue? o Initial medical triage? o Decontamination of ambulatory and non-ambulatory casualties? o Preserving scene and evidence? o Chain of custody documentation? o Recovery and reconstitution? • Can the FD meet travel and response times IAW DoDI 6055.06, *DoD Fire and Emergency Services (F&ES) Program*? • Does the FD possess a plume-modeling capability? • Does the Fire Chief or designated representative attend the ATWG and CBRNE WG? • Is the FD involved in developing AT exercise scenarios? • Are 911 operators trained/certified Public Safety Telecommunicator's IAW NFPA 1061? • Are installation grid maps posted, current, and acurate?	DoD Std 20 DoDI 2000.18, Guideline 3 Strategic Goal 2D
EM-PLN-09	**SECURITY FORCES (SF) TERRORIST INCIDENT RESPONSE (TIR) MEASURES** • Does SF TIR SOPs address: o Establishing C3 consistent with the NMS and ICS? o Securing a perimeter around CBRNE/HAZMAT incident? o Initiating evacuation or shelter-in-place actions? o Establishing entry/exit traffic control points? o Establishing safe routes for emergency vehicles? o Considerations for a secondary device? o Searches for secondary devises conducted in conjunction with EOD team members? o Scene, evidence preservation, and chain of custody? • Are procedures established to verify/permit entry of emergency response vehicles onto the installation during higher FPCONs? • Does SF personnel receive incident response training i.e., Terrorist Incident Response, HAZMAT Awareness, IED recognition, etc.? • Are SF dispatch operators trained and certified? • Are installation grid maps posted, current, and acurate?	DoD Std 20 DoDI 2000.18, Guideline 3 Strategic Goal 2D
EM-PLN-10	**MEDICAL (MED) TERRORIST INCIDENT RESPONSE (TIR) MEASURES** • Does the installation possess a mass casualty (MASCAL) response capability? • Where does emergency medical response come from; installation fire	DoD Std 20 DoDI 2000.18, Guideline 3

	department, clinic/hospital, local community, host-nation? • 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)? • How many ambulances are available from the installation and local community to support a MASCAL incident within the first hour (golden hour)? o What level are ambulances equipped; basic life support (BLS) or advanced life support (ALS)? • Is helicopter medical evacuation available? o Where does it come from and what is the response time? • What type of communications (radios, cell phones, pagers) do medical first responders possess? o Is this equipment adequate? • Are MASCAL response kits available and ready? o How many casualties will each kit support? • Are installation grid maps posted, current, and accurate?	Strategic Goal 2D
EM-PLN-11	**EXPLOSIVE ORDNANCE DISPOSAL (EOD) TERRORIST INCIDENT RESPONSE (TIR) MEASURES** • Does the installation have an EOD team assigned? If not, where does EOD support come from? • Is this support available 24/7? • Are EOD notification procedures developed? • What is the EOD response time? • Has the supporting EOD team reviewed the installation bomb threat/search plan? • Has EOD conducted a site survey and become familiar with the installation? • Are installation grid maps posted, current, and acurate? • Does EOD provide IED recognition, bomb threat/search classes? • Does a EOD representative attend the ATWG? • Is EOD involved in developing scenarios for AT exercises? • What type of communications does EOD possess? o How is communication interoperability conducted between EOD and other installation responders, EOC? • Does the installation have communication connectivity with responding EOD teams? (most EOD teams have cellular phones) • Does EOD have access to SIPRNet?	DoD Std 20 DoDI 2000.18, Guideline 3 Strategic Goal 2D
	Terrorist Consequence Management Measures. Installation commanders shall include Terrorist Consequence Management, CBRNE and public health emergency preparedness, and emergency response measures as an adjunct to the overall AT Plan. These measures shall focus on mitigating vulnerabilities of DoD personnel, families, facilities, and materiel to terrorist use of WMD and CBRNE weapons, as well as overall disaster planning and preparedness to respond to a terrorist attack. These measures shall include integration and full compliance with DoD Emergency Responder guidelines (DoDI 2000.18), mass notification system standards (UFC 4-021-01), establishment of medical surveillance systems (DoDD 6490.2), and deployment of CBRNE sensors and detectors; providing collective protection, and providing individual protective	DoD Std 21 E3.21.1

	equipment in the following priority; emergency and first responders; critical personnel; essential personnel; and other personnel. Develop and implement site-specific CBRNE preparedness and emergency response measures that are synchronized with a corresponding FPCON measure. Establish MAAs or other similarly constructed protocols with the appropriate local, State, Federal, or host-nation authorities to support AT Plan execution and augment incident response and post-incident consequence management activity. Ensure the installation can warn its resident population in affected areas of CBRNE hazard identification immediately, but no longer than 10 minutes after detection. The warning must include instructions to remain in place or evacuate. Develop and implement site-specific public health emergency response measures that are synchronized with FPCON levels IAW DoD Drinking Water Policy and DoDD 6490.2.	
EM-PLN-12	**CBRNE EMERGENCY RESPONSE PROGRAM** • Has the installation commander designated in writing a commissioned officer, non-commissioned officer, or civilian staff officer as the Emergency Disaster Planning Officer (EDPO) with CBRNE emergency response program management responsibilities? o Does the EDPO coordinate the CBRNE Emergency Response Plan? o Does the EDPO coordinate with local authorities, emergency manager, Local Environmental Planning Committee, EOC, etc.? o Is the EDPO a member of AT Working Group (ATWG)? • Has the EDPO established a CBRNE Emergency Response WG? o Is this group responsible for planning, assessing, training, and exercising the installation CBRNE program? [can consist of members from the ATWG] o Has this group developed a CBRNE VA? • Has an annual assessment of the CBRNE Emergency Response Program been conducted? • Does the EDPO maintain a current inventory list of all emergency response equipment on the installation as well as what is available by mutual aid assistance through local communities/HN? • Has the installation received emergency response equipment through the Guardian Installation Protection Program (PPE, detection equipment, decontamination equipment, mass notification system, etc.)? o Is this equipment included in the installation emergency response equipment inventory list? o Is equipment utilized, secured and accounted for, shelf-life tracked, available for immediate use, and maintained and inspected?	DoD Std 21 DoDI 2000.18, Guideline 2 Strategic Goal 2D
EM-PLN-13	**CBRNE EMERGENCY RESPONSE PLAN** • Has a CBRNE Emergency Response 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	DoD Std 21 DoDI 2000.18, Guideline 2

	the AT Plan] • Is the plan adequately staffed, exercised, and signed by commander? • Does the plan contain specific procedures first and emergency responders must follow for CBRNE incidents? • Has detailed SOPs been developed by each organization tasked to support the plan? (FD, SF, MED, EOD, PAO, mailroom, etc.) • Does the plan identify who is responsible for sampling, packaging, and chain of custody of CBRNE materials? • Do procedures describe who, what, when, where, and how these processes are conducted? • Are personnel trained and certified to conduct these operations? • Does the plan address search procedures for secondary devices? • Has EOD coordinated / approved search procedures? • Are plume modeling procedures addressed in the plan? • Do procedures describe who, what, when, where, and how plume modeling is conducted? • Do procedures describe how the most current weather data is provided to the Incident Commander? • Is the installation aware of the reach-back capability to request plume modeling through DTRA's Operations Center at o Comm: (703) 767-2118? o DSN: 427-2118 • Has a list of toxic industrial materials/toxic industrial materials (TIC/TIM) located on the installation and surrounding community been developed? [must be included in the local CBRNE TA] • Does the list identify type, quantity, location, etc.? • Does the Fire Department and EOC possess a current copy? • Are procedures developed to implement site-specific CBRNE preparedness and emergency response measures that are synchronized with a corresponding FPCON level? • Is there a plan to request contract for a clean-up/restoration crew after a HAZMAT or CBRN event? • Does the 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]	& 4 DoD O-2000.12-H, Ch. 11 Strategic Goal 2D National Response Plan (NRP)
EM-PLN-14	**MASS CASUALTY (MASCAL) PLANNING** • Has a MASCAL Plan been developed? o Is this a stand-alone plan or included in the AT Plan? • Does the plan describe how emergency responders (SF, FD, MED) from the installation, local community, or host nation (HN) respond to MASCAL incidents? • Is the plan current, exercised, and signed by the commander? • Does the plan identify what constitutes a MASCAL incident for the installation; 2, 4, 6, personnel? • Does the MASCAL Plan address: • Incident command and organization of responders • Recall procedures? • Medical facility capabilities for the installation, local community, or HN? (Level of care, specialty, bed space, etc.)	DoD Std 21 DoDI 2000.18, Guideline 3 Strategic Goal 2D, 2G

	• Installation medical team duties, responsibilities, and composition? • Installation medical control center (MCC) operations? • Communications capabilities (radios, cell phones, etc.) and interoperability with responders • Response after duty hours when medical facility is closed or minimally manned? • MASCAL flow diagram? • Securing medical facility following a CBRNE incident? • Bomb threat, evacuation, and shelter-in-place procedures? • Resources available to provide first response, triage, transportation, casualty classification and tracking, and personnel accounting? • MASCAL training and exercise requirements? • Medical surveillance for illness resulting from a biological agent? • Identify number of ground and air-ambulances available from installation, local community, or HN to support a MASCAL incident? • Identify which medical care equipment will be taken with medics responding to the MASCAL, i.e., airway management bag, oxygen delivery system, trauma bag, ALS medication bag? • Mortuary affairs functions and include fatality management and contaminated casualty and/or remains handling, decontamination, transportation, and temporary storage? • Are MOU / MOAs established with the local community or HN medical facilities and are they current?	
EM-PLN-15	**FIRE DEPARTMENT (FD) EMERGENCY RESPONSE EQUIPMENT** **FD PERSONAL PROTECTIVE EQUIPMENT (PPE):** • What level of CBRNE / HAZMAT operational capability has the FD established; Operations Level, Technician Level? • Are fire fighters trained and certified under the FF Certification System to the appropriate HAZMAT level to meet the established department operational capability? • What HAZMAT level are fire fighters trained to; Awareness, Operations, Technician, Incident Command (IC)? o Are certifications current and documented? • Do FD personnel possess PPE for response to CBRN/HAZMAT incidents based on the FDs 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 • Are respirators CBRN approved by the National Institute for Occupational Safety and Health (NIOSH)? • Are personnel who wear PPE trained and certified IAW Occupational Safety and Health Administration (OSHA) 29 Code of Federal Regulations (CFR) 1910.120, *Hazardous Waste Operations and Emergency Response* and 1910.134, *Respiratory Protection*? • Are personnel who wear NIOSH-certified respirators enrolled in a respiratory protection program? • Is there a current inventory of all PPE? • Is PPE serviceable and ready for immediate use?	DoD Std 21 DoDI 2000.18, Guidelines 3, 6, 7, & 9 Strategic Goal 2G

	• How is shelf-life equipment items tracked? **FD DETECTION AND DECONTAMINATION (DECON) EQUIPMENT:** • What type of detection/monitoring equipment does the FD possess for CBRN / HAZMAT incidents? • Is there a current inventory of all detection equipment? • How is detection equipment repaired or serviced? • Does the FD possess a plume-modeling capability? • 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), Reach-back capability (DTRA), etc. • Are SOPs developed for plume modeling? o Do procedures specifically describe who, what, when, where, and how plume modeling is conducted? o How does the IC receive accurate and current weather data? • Is the FD tasked to perform mass decon of victims following CBRNE / HAZMAT incidents? • What types of decon equipment does the FD possess? • Do FD SOPs describe who, what, when, where, and how mass decon is conducted? o Is guidance included in the CBRNE Emergency Response Plan? • Are MOU / MOA / MAAs established with the local community / HN if no decon capability exists? Are MOU / MOA / MAAs current and been exercised? • Is there a current inventory of all decon equipment? • How is shelf-life equipment items tracked? • How is equipent maintained?	
EM-PLN-16	**SECURITY FORCES (SF) EMERGENCY RESPONSE EQUIPMENT** **SF PPE:** • What level of operational capability has SFs established i.e., HAZMAT Awareness, Level C PPE, conduct cordon on the cold / warm zone, etc.? o Are SF personnel trained and certified to this level? o Are SF personnel appropriately equipped? • Do SF personnel possess PPE for response to CBRN incidents i.e., protective mask, rubber gloves, tyvek suit, etc.? o Are masks NIOSH approved? o For contracted civilian security forces / guards: (the statement of work has to state whether CBRN equipment, training, and certification or awareness course can be implemented • Are SF personnel who wear PPE trained and certified IAW OSHA 29 CFR 1910.120 and 1910.134? • Are personnel who wear NIOSH-certified respirators enrolled in a respiratory protection program? • Is there a current inventory of all PPE? • Is equipment serviceable and ready for immediate use? • How is shelf-life equipment items tracked?	DoD Std 21 DoDI 2000.18, Guidelines 3, 6, 7, & 9 Strategic Goal 2G

	• How is equipment maintained?	
EM-PLN-17	**MEDICAL (MED) EMERGENCY RESPONSE EQUIPMENT** **MED PPE:** • What level of operational capability has been established for medical responders i.e., HAZMAT Awareness/Operations, Level C PPE, patient decon? o Are they trained and certified to this level? o Are they appropriately equipped? • Are personnel who wear PPE trained and certified IAW OSHA 29 CFR 1910.120 and 1910.134? • Are personnel who wear NIOSH-certified respirators enrolled in a respiratory protection program • Do MED personnel possess PPE to transport decontaminated patients I.e., protective mask, tyvek suit, gloves, etc.? • Do MED personnel possess adequate PPE to conduct decon operations, if tasked? • Is there a current inventory of all PPE? • Is equipment serviceable and ready for immediate use? • How is shelf-life equipment items tracked? **MED DETECTION AND DECON EQUIPMENT:** • Does the MED decon team possess detection/monitoring equipment for CBR incidents? • How is detection equipment repaired or serviced? • Does the installation hospital/clinic possess a decon capability? • Does the decon capability meet or exceed the standards set forth by the National Fire Protection Agency (NFPA) 472, Joint Commission on Accredidation of Healthcare Organizations (JCAHO) E.C.1.4., or Service directed requirement? • Do SOPs clearly describe who, what, when, where, and how in-place patient decon is conducted? o Are these procedures in the MASCAL Plan or stand-alone plan? • Are decon team members trained and is training documented? • Is there an inventory of all decon equipment? o Is equipment serviceable and ready for immediate use? o How is shelf-life equipment items tracked? • Has a decon site been pre-identified with run-off containment considered? • What are the methods adopted for victim decontamination? • Are MOU/MOAs established with local/HN medical facilities who will accept contaminated patients? • Are procedures established for transporting decontaminated casualties from the incident site to the nearest medical facility? • Do ambulances have patient covers and blankets for ambulatory and litter patients after the decontamination process? • For installations with contract ambulance services, are WMD/CBRNE planning considerations required of the EMS included in the contract statement of work?	DoD Std 21 DoDI 2000.18, Guidelines 3, 6, 7, & 9 Strategic Goal 2G

	• Are antidote injectors (i.e. CANA and NAAKs) or pharmaceuticals and vaccines available?	
EM-PLN-18	**EXPLOSIVE ORDNANCE DISPOSAL (EOD) EMERGENCY RESPONSE EQUIPMENT** **EOD PPE:** • What level of operational capability has EOD established (HAZMAT Operations, Technician Level)? o Are EOD technicians trained and certified to this level? o Are they appropriately equipped? • Do EOD personnel possess adequate PPE for CBRNE response (i.e. Level A, B, C, self-contained toxic environment protective outfit (STEPO), bomb suit, etc.? • Are SCBA respirators CBRN approved by NIOSH? • Is there an inventory of all PPE? • Is equipment serviceable and ready for immediate use? • How is shelf-life equipment items tracked? • How is equipment maintained? • Are personnel who wear PPE trained and certified IAW OSHA 29 CFR 1910.120 and 1910.134? • Are personnel who wear NIOSH-certified respirators enrolled in a respiratory protection program? **EOD DETECTION EQUIPMENT:** • What type of detection/monitoring equipment does EOD possess for CBR incidents? (If none, is there coordination with FD or HAZMAT team to use or augement needed equipment?) • Is there a current inventory of all detection equipment? • How is detection equipment repaired or serviced?	DoD Std 21 DoDI 2000.18, Guidelines 3, 6, 7, & 9 Strategic Goal 2G
EM-PLN-19	**MAIL FACILITY RESPONSE MEASURES** • Does the mail facility SOP address actions for mail handlers to take upon encountering a suspicious envelope or package? o Isolating the envelope / package o Securing the area o Isolate / shutoff HVAC or air handling systems / equipment o Evacuating the facility / quarantine potentially exposed personnel o Notifying emergency responders o Conducting personnel decontamination if warranted i.e., washing hands with warm soapy water o Donning personnel protective equipment (NIOSH approved respiratory protection mask and nitrile / vinyl or other OSHA approved gloves) o Are personnel trained and exercised in the use of issued PPE? o Are personnel exercised periodically on procedures for responding to the discovery of a suspicious envelope or package?	DoD Std 21 US Postal Service Publication 166 DoD O-2000.12-H, App 19 COCOM AT OPORD
EM-PLN-20	**COMMUNICATIONS** • Is a Communications Annex included in the AT Plan? • Does this annex address: o Communication capabilities, redundancies, and limitations? o Installation mass notification systems (MNS)? o Installation 911 system?	DoD Std 21 DoDI 2000.18, Guideline 6

	○ Land mobile radio (LMR) systems used by first responders and interoperability with local community ○ Location of repeaters, identification of areas not covered by LMRs, and workarounds for emergencies in such area? • Do installation first responders (SF, Fire, Medical, EOD, etc.) have adequate LMR communications? ○ Can first responders communicate effectively between each other via LMR i.e., SF to FD, FD to MED? ○ Can installation first responders communicate effectively via LMRs with local responders? ▪ What work-arounds are used when LMRs are not interoperable? ○ Do LMRs provide adequate coverage on the installation? ▪ Are there any dead spots? ▪ Are radios on a trunked system? ▪ Are radios capable of secure communications? • Is the system narrow-band compliant?	Strategic Goal 2G, 2I
EM-PLN-21	**MASS NOTIFICATION SYSTEM (MNS)** • Does the installation have a MNS capability that meets the criteria in the Unified Facilities Criteria (UFC) 4-021-01, *Design and O&M: Mass Notification Systems*? [mass notification is the capability to provide real-time information to all building occupants or personnel in the immediate vicinity of a building during emergency situations] • Does the installation use the types of MNSs described in the UFC e.g., Individual Building System, Giant Voice, and Telephone Alerting System? ○ What other systems does the installation use to conduct mass notification i.e., email pop-up, commander's channel, radios, etc.? • Is each installation MNS addressed in the Communications Annex to the AT Plan? ○ Does guidance describe who, what, when, where, and how each MNS is used? ○ Are maintenance procedures and testing requirements addressed? • Can the installation warn populations in affected areas of a CBRNE hazard immediately, but no longer than 10 minutes after detection? [DoDI 2000.16 and COCOM requirement] • Do all new inhabitated buildings possess a MNS capability? ○ Inhabitated buildings are buildings or portions of buidlings 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 • Do all new primary gathering buildings possess a MNS capability? ○ Primary gathering buildings are inhabitated buildings routinely occupied by 50 or more DoD personnel • Do all new billeting buildings possess a MNS capability? ○ Billeting is any building or portion of a building, regardless of population density, in which 11 or more unaccompanied DoD personnel are routinely housed, including Temporary Lodging Facilities and military housing permanently converted to unaccompanied housing	DoD Std 21 Strategic Goal 2I UFC 4-021-01
EM-PLN-22	**EVACUATION AND SHELTER-IN-PLACE (SIP)** • Is evacuation and SIP guidance developed and included in the AT Plan? ○ Do procedures describe who, what, when, where, and how evacuation and SIP is conducted?	DoD Std 21 E3.21.1.

	o Do procedures describe the various MNSs used to conduct evacuations and SIP? o Are evacuation / SIP scenarios included in AT exercises? • Has SIP procedures been developed for each facility on the installation? o Do procedures address shutting down HVAC systems, exhaust fans, closing / taping windows / doors, relocating to higher floors or interior windowless rooms, establishing lines of communication to maintain situational awareness, etc.? o Are facility personnel trained to conduct SIP? o Do procedures describe how SIP announcements are disseminated throughout the facility? • Is evacuation and SIP guidance provided to installation personnel and housing residents? • 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] o Do procedures describe who is authorized and qualified to issue evacuation or SIP instructions (Fire Department, Security Forces, etc.?	Strategic Goal 2D, 3F
EM-PLN-23	**PUBLIC AFFAIRS OFFICER (PAO)** • Are PAO roles and responsibilities in supporting the AT Program described in the AT Plan? • Has procedures been developed for releasing information on terrorist events? • Do procedures identify personnel to respond to the scene, escort media, and run media center? • Do PAO personnel have adequate communications? (radio/cell phone/pager) • Has a facility been identified to serve as the Joint Information Bureau (JIB) to brief media in the event of an incident? o Has an alternate JIB been identified? o Does the JIB have back-up power if required? • Does the PAO work with the installation Webmaster to review all material prior to being posted on the installation Internet Website? • Is there a process to ensure exploitable material is not posted on any websites on the installation? • Does the PAO review the installation's local newspaper? • Is the PAO part of the ATWG? • Is the PAO involved in installation AT exercises? • Has AT articles been published in the paper and what frequency?	DoD Std 21 DoDI 2000.18, Guideline 3 DoD O-2000.12-H, Chapter 19 Strategic Goal 2D
EM-PLN-24	**MEMORANDUM OF UNDERSTANDING (MOU), MEMORANDUM OF AGREEMENT (MOA), AND MUTUAL AID AGREEMENT (MAA)** • Has MOU / MOA / MAAs been developed with the local community or host-nation to ensure CBRNE emergency response capabilities are integrated into installation's CBRNE Emergency Response Plan? • Are agreements established with local emergency responders? • Are all MOU / MOA / MAAs reviewed annually and modified when and where appropriate? • Is there a POC who maintains and tracks all AT related MOU / MOA / MAAs for the installation?	DoD Std 21 DoDI 2000.18, Guideline 2 Strategic Goal 2H

	• Does the Status of Forces Agreement provide for emergency response?	
EM-PLN-25	**Force Protection Conditions.** 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). • Has specific guidance been developed to implement the following FPCON measuress on the installation? o Measure ALPHA 5: Initiate food and water operational risk management procedures, brief personnel on food and water security procedures, and report any unusual activities o Measure ALPHA 6: Test mass notification system o 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 o 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 o 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	DoD Std 22 E3.22.2. & Enclosure 4 Strategic Goal 2D
3. AT TRAINING AND EXERCISES		

EM-TE-01	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. 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. 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.	DoD Std 23 E3.23 DoDI 2000.18, Guideline 5 Strategic Goal 3F
	• Has the ATO developed an AT Training and Exercise Program and included guidance in the AT Plan or referenced its location? • Does the installation training program provide for the necessary initial and periodic refresher training, consistent with the threat, appropriate to the different emergency responsibilities? • Is AT training incorporated into unit-level training plans and pre-deployment exercises? • Has the installation established a CBRNE Emergency Response Training program? (Training should be consistent with 29 CFR 1910.120, *Hazardous Waste Operations and Emergency Response*, National Fire Protection Association (NFPA) 472, *Standard for Professional Competence of Responders to HAZMAT Incidents* and NFPA 473, *Standard for Competencies for EMS Personnel Responding to HAZMAT Incidents*, appropriate governing Federal, State, or HN regulations, etc.) • Does the annual AT exercise encompass all aspects of AT Plan and associated plans? • Are exercise scenarios based on the installation local Threat Assessment (TA) including CBRNE? • Is the Design Basis Threat (DBT) exercised? • Are Terrorist Incident Response and Terrorist Consequence Management measures exercised? • Are mass casualty (MASCAL) exercises conducted? • Is the current baseline FPCON through FPCON CHARLIE exercised by the installation and separate facilities? • Is FPCON DELTA implemented at parts of the installation? • Are evacuation and shelter-in-place (SIP) procedures exercised? • Are after action reports and lessons learned developed? • Is AT exercise documentation maintained for at least 2 years?	

4. AT RESOURCE APPLICATION		
EM-RA-01	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 approved methodology for documenting and prioritizing AT resource requests. • Has the ATO developed a process for requesting AT funds to mitigate equipment shortfalls of the CBRNE Emergency Response Program and annual CBRNE VA? [Coordinate with Security Operations] • Does the EDPO maintain a current list of CBRNE equipment shortfalls?	DoD Std 30 E3.30.1. DoDI 2000.18, Guideline 1 Strategic Goal 4A
5. AT PROGRAM REVIEW		
EM-PR-01	Installation commanders 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 AT Programs comply with the standards prescribed in DoDI 2000.18. AT Program Reviews shall evaluate all mandatory AT program elements (see DoD Standard 1) and assess the viability of AT Plans (see DoD Standard 7) in view of local operational environment constraints and conditions.	DoD Std 31 E.3.31.1. DoDI 2000.18 Guideline 4
	• Is the commander conducting an annual review of the CBRNE Emergency Response Program to facilitate program enhancement and to ensure compliance with DoDI 2000.16 Standards and DoDI 2000.18 Guidelines? • Does the program review evaluate the installation's ability to respond to a CBRNE event? • Is the Defense Continuity Program part of the program review?	Strategic Goal 5C