UNITED STATES NORTHERN COMMAND
(USNORTHCOM)

USNORTHCOM
Antiterrorism (AT) Operations Order (U)
05-01

6 May 2005

For Official Use Only

HEADQUARTERS, US NORTHERN COMMAND
060800TMAY05

USNORTHCOM OPORD 05-01 (U)
ANTITERRORISM (AT) OPERATIONS ORDER (U)

(U) References.

a. (S) Unified Command Plan, 1 March 2005 (U).

b. (S/NF) Forces For Unified Command FY 2004, December 19, 2004 (U).

c. (S) USNORTHCOM CONPLAN 2002 Homeland Defense (Draft) (U).

d. (U) EXORD for Standup of USNORTHCOM CONUS AT-FP Responsibility, DTG 071710Z MAY 04.

e. (U) United States Northern Command Concept of Operations, March 1, 2004.

f. (U) USNORTHCOM Antiterrorism Program/Force Protection Concept of Employment for CONUS, 1 September 2004.

g. (U) National Response Plan, December 2004.

h. (U) National Incident Management System, DHS, March 1, 2004.

i. (U) Homeland Security Presidential Directive/HSPD-5, Management of Domestic Incidents, February 28, 2003.

j. (U) Executive Order 12333, United States Intelligence Activities, December 4, 1981.

k. (U) Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, November 1988.

l. (U) Executive Order 13354, National Counterterrorism Center, August 27, 2004.

m. (U) Executive Order 13355, Strengthening Management of the Intelligence Community, August 27, 2004.

n. (U) Executive Order 13356, Strengthening the Sharing of Terrorism Information to Protect Americans, August 27, 2004.

o. (U) DoD Directive 2000.12, DoD Antiterrorism/Force Protection Program, August 18, 2003.

p. (U) DoD Directive 3020, Defense Critical Infrastructure Protection (Draft).

q. (U) DoD Directive 4500.54, Official Temporary Duty Travel Abroad, May 1991.

r. (U) DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations Not Affiliated with the DoD, January 7, 1980.

s. (U) DoD Directive 5210.56, Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties, November 1, 2002 (Change 1, January 24, 2002).

t. (U) DoD Directive 5210.84, Security of DoD Personnel at US Missions Abroad, January 22, 1992.

u. (U) DoD Directive 5240.1, DoD Intelligence Activities, April 25, 1988.

v. (U) DoD Regulation 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, December 1982.

w. (U) DoD Instruction 2000.16, DoD Antiterrorism Standards, June 14, 2001.

x. (U) DoD Instruction 2000.18, DoD Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines, December 4, 2002.

y. (U) DoD Instruction 5105.57, Procedures for the US Defense Representative (USDR) in Foreign Countries, December 1995.

z. (U) CJCS Instruction 5261.01C, Combating Terrorism Readiness Initiatives Fund, April 1, 2003.

aa. (U) CJCSM 3150.03B, Joint Reporting Structure Event and Incident Reports, July 28, 2003.

bb. (U) DoD Handbook 2000.12-H, DoD Antiterrorism Handbook, February 9, 2004.

cc. (U) DoD 4500.54-G, “DoD Foreign Clearance Guide,” Electronic version available online at http://www.fcg.pentagon.smil.mil/fcg/fcg.html.

dd. (U) Unified Facilities Criteria (UFC) 4-010-01, Design: DoD Minimum Antiterrorism Standards for Buildings, October 8, 2003.

ee. (U) Joint Publication 0-2, Unified Action Armed Forces, July 10, 2001.

ff. (U) Joint Publication 3-40, Joint Doctrine for Combating Weapons of Mass Destruction, July 8, 2004.

1. (U) Situation.

a. (U) USNORTHCOM has been assigned the Force Protection (FP) mission and AT Program responsibility for the USNORTHCOM AOR. The purpose of the FP mission is to defend, detect, and mitigate against terrorist attacks directed at DoD personnel, infrastructure, resources, and information to ensure DoD's continued warfighting capability. The scope of this mission extends to all DoD Elements and personnel in the USNORTHCOM AOR, whether assigned or unassigned to USNORTHCOM. While the FP mission supports USNORTHCOM's primary missions of Homeland Defense (HLD) and Civil Support (CS), it is a separate task assigned in the Unified Command Plan (UCP) (*ref. a*.) and is executed through a different chain of command from the specified USNORTHCOM missions of HLD and CS. The successful execution of the USNORTHCOM FP mission enables the USNORTHCOM HLD and CS missions, and assures availability of DoD assets in support of other Combatant Command-assigned missions.

b. (U) Area of Concern.

(1) (U) Area of Responsibility (AOR).

(a) (U) USNORTHCOM's geographic AOR for the conduct of normal operations, contingency planning, security cooperation, and force protection is the 48 contiguous States and the District of Columbia, Alaska, Canada, Mexico, the Gulf of Mexico, the Caribbean Sea and its island nations and European possessions (including the Commonwealth of Puerto Rico, the U.S. and British Virgin Islands, Turks and Caicos Islands and Bermuda), and the Atlantic Ocean and its island nations and European possessions (excluding Greenland) within the area bounded by the Arctic Ocean from 169 degrees W east to 045 degrees W, south to 20 degrees N, west to 064 degrees W, south to 17 degrees N, west to 068 degrees W, north to 21 degrees N, west to 073 degrees W, southwest to 19 degrees N, 075 degrees W, west to 079 degrees W, north to 20 degrees N, west to Mexico, south from Mexico at 092 degrees W to 08 degrees N, west to 112 degrees W, northwest to 50 degrees N, 142 degrees W, west to 179 degrees W, northeast to 63 degrees N, 173 degrees W, northeast to 64 degrees N, 169 degrees W, and north to 90 degrees N. U.S. Southern Command (USSOUTHCOM) provides contingency planning, operations, security cooperation, and force protection for the Bahamas and Cuba, and their territorial waters (*ref. a*.).

(b) (U) As addressed in this order, the CONUS portion of the USNORTHCOM AOR comprises the contiguous 48 States, the District of Columbia and Alaska. The OCONUS portion of the USNORTHCOM AOR comprises the Commonwealth of Puerto Rico, Canada, Mexico, Bermuda, the U.S. and British Virgin Islands, Turks and Caicos Islands, and St. Pierre and Miquelon Islands.

(c) (U) Within the USNORTHCOM AOR two Joint Operations Areas (JOA) have been established: Alaska and the National Capital Region (NCR).

1. (U) The Alaska JOA comprises the landmass of the State of Alaska.

2. (U) The NCR comprises the geographic area located within the boundaries of the District of Columbia; Montgomery and Prince Georges Counties in the State of Maryland; Arlington, Fairfax, Loudoun, and Prince William Counties and the Cities of Alexandria, Fairfax, Manassas and Manassas Park in the Commonwealth of Virginia; and all cities and other units of government within the geographic areas of such District, Counties and City. (*DoD Instruction 5305.5, Space Management Procedures, National Capitol Region, June 14, 1999*)

(2) (U) Area of Interest. USNORTHCOM's area of interest includes the entire globe, as operations throughout the world that require U.S. infrastructure, C4ISR and power projection capabilities that reside in USNORTHCOM's AOR. USNORTHCOM will request support from other Combatant Commanders, Services and Agencies, when a threat is detected in the USNORTHCOM AOR. USNORTHCOM must also establish and maintain meaningful and effective bi-lateral or multi-lateral security relationships with countries in USNORTHCOM's AOR to coordinate security and defense issues of mutual concern. As necessary, our regional partners will track the HLD threat, share threat information and intelligence, and facilitate threat engagement by USNORTHCOM *((S) USNORTHCOM CONPLAN 2002 Homeland Defense (Draft) (U))*.

a. (U) Within CONUS, USNORTHCOM's Area of Interest extends to those critical non-DoD events and infrastructure that may impact DoD operational capabilities or require DoD support for protection or incident management support.

c. (U) Deterrent Options. N/A.

d. (U) Enemy Forces. *Annex B, Intelligence*. USNORTHCOM faces a wide range of potential threats in executing its command responsibilities. These threats range from strategic and regional threats posed by nation states to threats from transnational and indigenous terrorist groups and criminal activities subject to federal law, regulation, and the Posse Comitatus Act. USNORTHCOM is responsible for protecting against the full range of threats to DoD assets within the USNORTHCOM AOR.

e. (U) Friendly Forces. *Annex A, Task Organization*.

(1) (U) USNORTHCOM Mission. USNORTHCOM conducts operations to deter, prevent and defeat threats and aggression aimed at the United States, its territories and interests within the assigned AOR. As directed by the President of the United States (POTUS) or Secretary of Defense (SECDEF), USNORTHCOM provides military assistance to civil authorities, including incident management operations.

(2) (U) The USNORTHCOM FP mission is coordinated with the following DoD offices:

(a) (U) The Secretary of Defense (SecDef).

(b) (U) The Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD (SO/LIC)).

(c) (U) The Assistant Secretary of Defense for Homeland Defense (ASD (HD)).

(d) (U) The Assistant Secretary of Defense for Health Affairs (ASD (HA)).

(e) (U) The Joint Staff J3 Deputy Director for Anti-Terrorism and Homeland Defense (DDAT/HD).

(3) (U) All DoD assets (assigned and unassigned) in the USNORTHCOM AOR are included in the FP mission execution.

(4) (U) In addition to DoD forces, USNORTHCOM coordinates within the Interagency to accomplish the FP mission.

(a) (U) Department of Homeland Security (DHS).

(b) (U) Department of State (DoS). Chiefs of Mission (COM) and for intelligence support.

(c) (U) Central Intelligence Agency (CIA).

(d) (U) U.S. Secret Service (USSS).

(e) (U) Other Primary Agencies (PA) for Special Security Events (SSE) and National Special Security Events (NSSE).

(3) (U) Throughout the AT OPORD the term DoD Elements is used to collectively refer to the Supporting Service Commanders (as defined in the Forces For, *ref. b*), the Supporting Subordinate Commands, the Supporting Defense Agencies and DoD Field Activities, and the Supporting Geographic and Functional Combatant Commands. (*Annex A*)

f. (U) Assumptions.

(1) (U) Terrorist organizations may target Government Agencies (GAs), DoD personnel, supporting personnel, their families, DoD installations' critical assets or infrastructure within the USNORTHCOM AOR.

(2) (U) DoD Elements and personnel could be at risk due to collateral damage when a terrorist organization targets civilian personnel or property throughout the USNORTHCOM AOR.

(3) (U) DoD Elements and personnel will coordinate U.S. military support with civilian security actions to provide necessary FP.

(4) (U) Implementing FP measures, AT training, and suspicious activity information collection will enhance our ability to disrupt terrorist surveillance/planning efforts.

(5) (U) Foreign Intelligence Services (FIS) of adversarial countries will continue to use all intelligence collection disciplines/capabilities at their disposal to collect information on U.S. capabilities, intentions, personnel, equipment and facilities. This is particularly significant for those countries providing support and assistance to terrorist groups or organizations.

g. (U) Legal Considerations.

(1) (U) Posse Comitatus. The Posse Comitatus Act (PCA) places limitations on military support to civilian law enforcement. The PCA is a criminal statute and violators are subject to fine and/or imprisonment. Prohibiting direct military involvement in law enforcement is in keeping with long-standing U.S. law and policy limiting the military's role in domestic affairs. However, there are statutory exceptions to the PCA's prohibitions and the statute does not limit the President's constitutional power to direct actions that might otherwise be prohibited by the PCA. For instance, the protection of DoD personnel, DoD equipment, classified military information or equipment, and official guests of the DoD, and such other actions that are undertaken primarily for a military or foreign affair's purpose are not prohibited. The PCA generally prohibits federal military personnel from interdicting vehicles, vessels and aircraft; conducting surveillance, searches, pursuit and seizures; or making arrests on behalf of civilian law enforcement authorities. The PCA applies to the federal uniformed services within DoD (Army, Air Force, Navy, Marines). It does not apply to the U.S. Coast Guard under Title 14, or the National Guard in State Active Duty and Title 32 status or to Title 5.

(2) (U) Intelligence Oversight. In accordance with Executive Order 12333, the DoD has established procedures in DoDD 5240.1 and DoD 5240.1-R for the collection, retention, and dissemination of information concerning U.S. persons. DoDD 5240.1 and DoD 5240.1-R apply to all DoD intelligence components and activities. The purpose of the procedures specified in DoD 5240.1-R is to enable DoD intelligence components to effectively carry out their authorized functions while ensuring that the privacy and other rights of U.S. persons are respected.

(3) (U) Acquisition of Information Concerning Persons and Organizations not affiliated with the DoD. DoDD 5200.27 establishes DoD policy and procedures governing the acquisition of information concerning persons and organizations, not affiliated with DoD, within the 50 States, District of Columbia, Puerto Rico, and U.S. territories and possessions. It applies to all DoD Elements other than the intelligence components subject to DoD 5240.1. DoD policy prohibits collecting, reporting, processing, or storing information on individuals or organizations not affiliated with DoD

except as provided by DoDD 5200.27. The collection of information essential to the protection of DoD functions and property, personnel security, and operations related to civil disturbance may be authorized under certain circumstances.

(4) (U) Definition of TACON (for Force Protection) (ref. n). TACON (for FP) enables the Geographic Combatant Commander to order implementation of FP measures (of which AT measures are integral) and to exercise the security responsibilities outlined in any respective MOA concluded under the December 1997 Department of State/Department of Defense MOU on the Security of DoD Elements and Personnel in Foreign Areas (known as the Universal MOU). Further, TACON (for FP) authorizes the Geographic Combatant Commander to change, modify, prescribe, and enforce FP measures for covered forces. This relationship includes the authority to inspect and assess security requirements and direct DoD activities to identify the resources required to correct deficiencies and to submit budget requests to parent organizations to fund identified corrections. The Geographic Combatant Commander can also direct immediate FP measures (including temporary relocation and departure) when, in his judgment, such measures must be accomplished without delay to ensure the safety of the DoD Personnel involved. Persons subject to the Geographic Combatant Commander's TACON (for FP) authority include not only active duty and Reserve component personnel in the Commander's AOR, but also, all DoD civilian employees and all family members in the AOR.

2. (U) USNORTHCOM AT Mission. Effective 1 October 2004, USNORTHCOM executes an AT Program to prevent and detect terrorist attacks against DoD personnel, their families, facilities, resources, installations, and infrastructure critical to DoD mission accomplishment as well as the preparation to defend against, and planning for the response to, the consequences of terrorist incidents in order to ensure continuation of essential DoD military operations in the USNORTHCOM AOR.

3. (U) Execution.

a. (U) Concept of Operation. USNORTHCOM will execute Tactical Control (TACON) (for Force Protection) (ref. n). This command relationship applies to all DoD personnel to include family members, DoD contractors and the Reserve Components, assigned or non-assigned. Day to day execution of the FP mission is the responsibility of the four Service Headquarters designated points of contact (POC), the eighteen Defense Agencies and DoD Field Activities Headquarters, and the six Combatant Command Headquarters located in the USNORTHCOM AOR. IAW references c, and d, of this OPORD, FP will be executed through the DoD Elements existing FP programs and current chains of command. USNORTHCOM will execute Geographic Combatant Command FP responsibilities through the five AT program elements and ten supporting tasks derived from references c, d, and e.

(1) (U) Commander’s Intent. The purpose of the USNORTHCOM AT Program is to prevent, detect, deter, defend, defeat and, if necessary, mitigate the effects of terrorist plans and operations in order to preserve the mission capability of forces

operating in the USNORTHCOM AOR. USNORTHCOM's ability to assess the threat and the current security posture of the USNORTHCOM AOR, to integrate USNORTHCOM efforts with those of the DoD Elements, DHS and DoS, and when required, to influence those actions to deter, prevent and defeat potential threats, are inherent in USNORTHCOM's FP responsibilities. The FP responsibilities and AT Program are critical to USNORTHCOM's success as a Geographic Combatant Command.

(a) (U) Execution of the AT Program in support of USNORTHCOM's FP responsibilities is the means through which USNORTHCOM will integrate the supporting mission areas and programs of FP, obtain situational awareness (SA) on the threat to the AOR, and influence FP Conditions (FPCON), as required. The intent of the USNORTHCOM AT Program is twofold. First, USNORTHCOM will work through existing DoD Elements' programs; serve as a bridge between the separate programs to create efficiencies and eliminate the vulnerabilities, gaps, and seams in our overall security posture. This includes off-installation security of DoD assets, personnel, infrastructure and operations and forces transiting or operating in the USNORTHCOM AOR. Second, focus on how USNORTHCOM ties in existing DoD FP responsibilities/actions with DHS, DoS, and local/HN civilian communities, to ensure interoperability and emergency preparedness.

(b) (U) End State: Effective integration of USNORTHCOM's FP responsibilities and AT Program with those of the DoD Elements in the USNORTHCOM AOR providing a synchronized defensive strategy protecting DoD assets against terrorist threats and ensuring DoD's capability for sustainment of critical operations.

(2) (U) General. This order provides procedures for planning, implementation, and execution of the USNORTHCOM AT Program as it pertains to the USNORTHCOM AOR in accordance with (IAW) DoD Directive 2000.12 (ref. n), DoDI 2000.16 (ref. w.), and DoDI 2000.18 (ref. x).

(a) (U) Purpose. The purpose of this OPORD is to specifically address the requirements, procedures, and instructions that will be implemented to execute the FP responsibilities and AT Program for the USNORTHCOM AOR.

(b) (U) The AT C2 relationship is TACON (for FP). The authority to establish this command relationship is DoDD 2000.12 and the EXORD for Standup of USNORTHCOM CONUS AT-FP Responsibility, 071901Z May 04, signed by the SecDef (reference d). USNORTHCOM's FP authorities for Title 32 forces will be handled on a case-by-case basis through EXORDs, DEPORDs, etc.

(c) (U) USSOUTHCOM retains FP responsibility for Cuba and the Bahamas, even though these islands are in the USNORTHCOM AOR. Per the USNORTHCOM-USSOUTHCOM Command Arrangement Agreement, JIATF-S forces operating across AOR lines will adhere to the FP guidance of the AOR in which they are located.

(3) (U) Commander, USNORTHCOM. Commander, USNORTHCOM has overall FP responsibility for all DoD assets in the USNORTHCOM AOR. Commander, USNORTHCOM is the supported Commander for all FP and AT actions. AT program elements and supporting critical tasks are:

(a) (U) Implement effective AT risk management processes and ensure the timely flow of information, intelligence/counter-intelligence, law enforcement information, and a common operational picture in the USNORTHCOM AOR. *Annex C, Appendix 1.* Supported by the following critical task:

(b) (U) Develop and execute theater AT plans, policies and programs. Supported by the following critical tasks:

1. (U) Establish AT policy, standards, and training requirements.

2. (U) Establish security requirements and FPCON.

3. (U) In-transit security and force tracking.

4. (U) CBRNE preparedness.

5. (U) Logistics support for AT.

(c) (U) Establish a theater AT training and exercise program. *Annex C, Appendix 3*.

(d) (U) Develop a theater Risk Management program that optimizes the planning, programming, and execution of resources, including Research, Development, Test and Evaluation (RDT&E) in support of the USNORTHCOM AT program. *Annex C, Appendix 7.*

(e) (U) Develop a theater risk management program that provides a holistic approach to theater level security assessments and comprehensive reviews of antiterrorism programs to ensure compliance with AT program standards. *Annex C, Appendix 6.*

1. (U) Vulnerability Assessments.

2. (U) Critical Infrastructure Protection.

b. (U) Tasks.

(1) (U) FP Responsibilities for Combatant Commands with Assigned Forces and Headquarters in CONUS with the exception of JOA-AK. The following paragraphs address the responsibilities of the Combatant Commands with assigned elements in CONUS (with the exception of USCENTCOM whose AT/FP program comes under

McDill AFB). USNORTHCOM has overall AT responsibility within the USNORTHCOM AOR. The Combatant Commands that have assigned elements stationed in CONUS will continue to exercise their Combatant Command AT responsibilities in accordance with their FP policies and programs. Nothing in this order changes the Geographic Combatant Commands' ultimate authority for AT and FP within their respective AORs nor the command authority over assigned forces. USNORTHCOM will exercise TACON (for FP) for the Combatant Commands' assigned personnel and USNORTHCOM Subordinate Service Commanders stationed in the USNORTHCOM AOR through their respective AT Programs. USPACOM, USSOUTHCOM, USSOCOM, USJFCOM, USTRANSCOM and USSTRATCOM will:

(a) (U) Establish AT policies and programs for assigned elements operating in or transiting through the USNORTHCOM AOR in coordination with USNORTHCOM AT policies and programs.

(b) (U) Ensure elements operating in CONUS, which are tenant units on Service installations, coordinate AT Programs and requirements with the host installation Commander.

(c) (U) Identify and provide USNORTHCOM with a list of designated incumbents of high-risk billets for assigned personnel in the USNORTHCOM AOR. Provide AT resident training to these personnel.

(d) (U) Submit emergent and/or emergency requirements in support of the Combatant Command mission to the CJCS for CbT RIF consideration and to submit AT requirements in support of AT Program as part of the PPBE process.

(e) (U) Coordinate all Joint Staff Integrated Vulnerability Assessments (JSIVA) through USNORTHCOM. NC/J34 will forward all requests for JSIVAs in the USNORTHCOM AOR to the Joint Staff. Other Combatant Commands will coordinate/manage their own internal assessment programs.

(f) (U) Identify areas and assets that are vulnerable to identified threat attack means and communicate these vulnerabilities to USNORTHCOM through the Core Vulnerability Assessment Management Program (CVAMP) module of the Antiterrorism Enterprise Portal (ATEP).

(g) (U) Include AT into all major exercise scenarios.

(2) (U) Supporting Service Headquarters, Defense Agencies and DoD Field Activities. Service Headquarters will execute their respective FP responsibilities and AT Programs IAW DoD and USNORTHCOM directives, and Service regulations and instructions. Defense Agencies and DoD Field Activities have responsibility to comply with the AT Program standards outlined in DoDI 2000.16 and will continue to execute existing AT Programs through their respective AT Program office or directorate. The

National Guard Bureau serves as the line of communication between USNORTHCOM and the National Guard of the States.

(a) (U) Develop implementing policies, standards and training requirements IAW *Annex C, Appendix 2*, to include:

1. (U) Establish standards for the assignment of Antiterrorism Officers (ATO), implementation of FPCON measures, and development and maintenance of comprehensive AT plans.

2. (U) Establish standards for AT physical security measures; and terrorist incident response and incident management measures.

3. (U) Establish AT training requirements.

4. (U) Commanders/Directors will develop AT and CBRNE exercises to test emergency response capabilities. The exercises need to be executed in conjunction with civilian counterparts where existing plans or MOAs exist that DoD Elements, local law enforcement, and civilian organizations will provide mutual support. Conduct AT exercises IAW *Annex C, Appendix 3*.

5. (U) Implement CBRNE installation preparedness measures IAW *Annex C, Appendix 9*.

6. (U) Implement a comprehensive assessment program IAW *Annex C, Appendix 6.*

7. (U) Establish in-transit security and force tracking procedures, and travel policies IAW *Annex C, Appendix 4*.

8. (U) Identify and submit a list of High Risk Personnel (HRP) billets to USNORTHCOM.

9. (U) Establish standards and procedures for waivers and deviations.

10. (U) Establish an off-installation housing policy for OCONUS locations.

11. (U) Submit PPBE and CbT RIF submissions IAW *Annex C, Appendix 7*.

12. (U) Comply with AT construction and contracting requirements IAW *Annex C, Appendix 8*.

13. (U) Implement USNORTHCOM CIP requirements IAW *Annex C, Appendix 10*.

(b) (U) Supporting Service Commanders will identify FP requirements, to include the National Guard.

(3) (U) Execution of the program elements are supported by the following USNORTHCOM assigned elements.

(a) (U) Joint Task Force – Alaska (JTF-AK). The USNORTHCOM AT Program and FP responsibilities will be executed through Commander, JTF – AK as the designated Joint Force Commander (JFC) for commands operating in or transiting the Alaska JOA. The JFC is the designated USNORTHCOM coordinating authority with HQUSPACOM and the USPACOM assigned forces stationed in, operating in, or transiting through Alaska regarding AT issues to ensure USPACOM AT concerns are adequately addressed. Commander, JTF – AK will:

1. (U) Establish and coordinate the FPCON in the Alaska JOA in accordance with USNORTHCOM directives and priorities.

2. (U) Coordinate intelligence support.

3. (U) Establish secure and robust communications with all forces and commands operating in or transiting the Alaska JOA.

(b) (U) Joint Force Headquarters - National Capital Region (JFHQ-NCR). When designated as JTF-NCR, JFHQ-NCR conducts response planning and coordination for land HLD and CS in the NCR JOA; and, as directed by USNORTHCOM, assumes control of DoD-assigned forces through the RFF process for execution of a specific mission within the NCR JOA.

1. (U) CDRJTFNCR retains AT/FP responsibilities for assigned/OPCON and/or TACON forces. Services retain AT/FP responsibilities for other forces within the JOA.

(c) (U) Joint Task Force – North (JTF-N). Execute IAW Annex C, Operations.

(d) (U) Joint Task Force – Civil Support (JTF-CS). Execute IAW Annex C, Operations.

(4) (U) Chiefs of Mission (COM). The COMs for Canada, Mexico, United Kingdom (for Bermuda, the Turks and Caicos Islands, and the British Virgin Islands) and France (for St. Pierre and Miquelon Islands) have security responsibility for the DoD Elements and personnel (including family members) specified in the respective Memorandum of Agreement (MOA) executed between Commander, USNORTHCOM and the COM.

(a) (U) MOAs are found on the USNORTHCOM J34 website on the SIPRNet portal at https://www.noradnorthcom.smil.mil/j3/j34/MOAs/Forms/AllItems.htm.

(b) (U) DoD Elements and personnel for which the COM has responsibility will be integrated with all other agencies represented at the Mission with regard to security briefings, personnel identification programs, residential surveys, and the Embassy Emergency Action Procedures (EAP).

(5) (U) United States Defense Representative (USDR). The USDRs for Canada, Mexico, United Kingdom (for Bermuda, the Turks and Caicos Islands, and the British Virgin Islands) and France (for St. Pierre and Miquelon Islands) will act as the focal point for planning, coordinating, and executing support to U.S. defense issues and activities that are not under the mission authority exercised by parent DoD Elements.

(a) (U) See *ref. p*, for a comprehensive list of USDR tasks and responsibilities.

(b) (U) Represents USNORTHCOM and other DoD Elements or personnel at country team meetings, such as the Emergency Action Committee (EAC) or other forums.

(c) (U) Be the USNORTHCOM point of contact for developing, coordinating, finalizing, and periodically reviewing the USNORTHCOM/COM MOA on AT issues. Monitors force size of DoD Elements or personnel in-country and reports changes to USNORTHCOM.

(d) (U) Ensure procedures are established to provide timely BLUE DART and similar threat warning information to DoD Elements and personnel under the COM. Work with the RSO in developing this system, using any notification systems already in place, such as the Warden program.

(e) (U) Supplement this OPORD as needed. Supplements may address service-specific requirements, but may not change the requirements established in this OPORD without authorization of USNORTHCOM.

(6) (U) National Guard Bureau (NGB). NGB will be the channel of communications for planning and coordinating with the National Guard (Air and Army National Guard) of the States when they are in a non-federalized status.

c. (U) Coordinating Instructions.

(1) (U) DoD Elements will report cases where implementation of AT guidance in this OPORD will adversely affect or significantly hamper accomplishment of their assigned duties. Waivers will be considered if compliance with the AT standard at a particular installation, site or facility will adversely affect mission accomplishment, exceed local capabilities, or require substantial expenditure of funds at a location where forces will be removed or relocated in the near future.

(2) (U) The primary venue to coordinate issues concerning policies, standards, and training requirements, will be through the USNORTHCOM Force Protection Coordination Committee (NC-FPCC) and the USNORTHCOM Force Protection Action Officer (NC-FPAO) Meeting. *Annex C.*

(3) (U) DoD personnel OCONUS will coordinate all AT and security matters using the United States Defense Representative (USDR) as a conduit to the Chief of Mission (COM). Issues should be elevated up the chain of command to the appropriate level (normally, the Service HQ or USNORTHCOM) specified in the terms of reference, instructions governing the mission, or this OPORD prior to affecting direct coordination with the COM.

(a) (U) DoD personnel who are under the security responsibility of a COM must meet standards developed by the USDR Overseas Security Policy Board (OSPB). If the standards developed by the USDR OSPB provide insufficient guidance for protection of DoD personnel, USNORTHCOM will work with the COM to augment the USDR security standards. The conflict resolution procedures in *ref. s* will be applied to resolve any questions regarding the applicability of USDR OSPB and/or DoD security standards.

(b) (U) To facilitate execution of this OPORD, USNORTHCOM and the DoD Elements will review existing MOAs at the appropriate level. Where agreements between DoD Element HQs and in-country agencies may be required to facilitate the execution of this order, consult NC/J34 before finalizing such agreements.

(c) (U) Organizations issuing travel orders must review USNORTHCOM/COM country MOAs to determine who has FP responsibility for the area in which personnel will be traveling. The designated responsible individual/agency for FP and their telephone numbers will be clearly listed on all TAD/TDY orders.

(4) (U) Coordinate with USNORTHCOM for FPCON changes.

(5) (U) Provide members to the NC-FPCC and FPAO meeting to address issues within the USNORTHCOM AOR.

(6) (U) Maintain awareness on the current country-specific threat assessments.

(7) (U) Submit reports IAW *Annex R, Reports*.

4. (U) Administration and Logistics.

a. (U) Concept of Support. Generally, FP logistics, personnel and other support policies and procedures are the same as those for other operations. Guidance for FP support planning and operations is available in applicable regulations, directives and Appendix 8 to Annex C. There are unique funding programs available in support of FP requirements for requesting those funds are identified in Appendix 7 to Annex C.

b. (U) Logistics Support for AT. *Refer to Annex C, Appendix 8.*

c. (U) Public Affairs. *Refer to Annex F.*

d. (U) Force Health Protection. *Refer to Annex C, Appendix 13*.

5. (U) Command and Control.

a. (U) Command Relationships.

(1) (U) Commander, USNORTHCOM. Commander, USNORTHCOM exercises TACON (for FP) for all DoD Elements and personnel within the USNORTHCOM AOR. USNORTHCOM AT responsibilities will be executed through the respective DoD Element's AT Program offices.

a) (U) Exercise TACON (for FP) over all DoD Elements and personnel (including FP responsibility for DoD family members and DoD contractors located on DoD installations/facilities) within the USNORTHCOM AOR (except those under the security responsibility of a COM). TACON (for FP) applies to all DoD personnel assigned permanently or temporarily, transiting through, or performing exercises or training in the USNORTHCOM AOR. TACON (for FP) applies to all forces within the USNORTHCOM AOR including those not assigned to USNORTHCOM. TACON (for FP) is in addition to the normal exercise of operational control (OPCON) over assigned forces by Commander, USNORTHCOM.

1. (U) Commander, USNORTHCOM has TACON (for FP) over all DoD personnel, facilities/locations, equipment, etc. in the USNORTHCOM AOR to include those of the Reserve Components.

2. (U) The Reserve Component of the Armed Forces of the United States are those Reserve members, units, and full-time support personnel of the Army National Guard of the United States (this does not include Title 32 personnel), the Army Reserve, the Naval Reserve, the Marine Corps Reserve, the Air National Guard of the United States, the Air Force Reserve (this does not include Title 32 personnel), and during time of war when directed by the President, the Coast Guard Reserve.

3. (U) USNORTHCOM exercises TACON (for FP) for the Reserve Component when members are performing a DoD mission or activity (e.g., such as inactive duty training or drilling for points; see however, the next paragraph concerning the National Guard).

(b) (U) The National Guard (Air National Guard and Army National Guard), in a non-Federalized State status (*i.e. Title 32 or State Active Duty (SAD)*, is not a Reserve Component. It is the intent of USNORTHCOM to enable the National Guard, in a State status, to comply with this OPORD by ensuring the National Guard receives

the proper information, guidance, funding, and other means necessary to achieve the objectives of this OPORD.

1. (U) Title 32 Personnel. During National Special Security Events (NSSE), or any other events designated by the SecDef, FP issues for Title 32 forces will be handled on a case-by-case basis through EXORDs, DEPORDs , etc. In circumstances where military personnel in a Title 10 or 32 status are working in close proximity, shared FP conditions and standards to ensure the security of all must be achieved. Separate FP standards for separate statuses are not only inappropriate but could result in endangering military personnel unnecessarily. USNORTHCOM will seek the cooperation of the States and Territories through the NGB and the Services to facilitate compliance with USNORTHCOM FP measures. Among other methods, such cooperative efforts may take the form of individual or collective memoranda of understanding and future regulations, instructions or directives.

2. (U) State Active Duty (SAD) Personnel. National Guard members performing SAD are under the command and control of the Governor, are paid with State funds, and perform missions directed by the Governor. Nevertheless, in a SAD status, National Guard personnel may also be working in close proximity with Active Duty or Title 32 personnel. When it is appropriate to seek standardized FP measures in these circumstances, USNORTHCOM will seek the cooperation of the States and Territories through the NGB and the Services to facilitate compliance with USNORTHCOM FP measures. Among other methods, such cooperative efforts may take the form of individual or collective memoranda of understanding. (See the following paragraph (para 3) concerning Federal facilities, installations, and equipment.)

3. (U) Because USNORTHCOM exercises TACON (for FP) for all DoD facilities/installations as well as DoD equipment in the USNORTHCOM AOR regardless of storage location, it is important for USNORTHCOM to work closely with the States and NGB to ensure that Federal facilities, installations, and equipment are properly protected. USNORTHCOM will coordinate with the States and Territories through the Services and National Guard Bureau as necessary to ensure that protection of Federal facilities, installations, and equipment meet DoD standards. Among other methods, such cooperative efforts may take the form of individual or collective memoranda of understanding and future regulations, instructions or directives.

(c) (U) USNORTHCOM TACON (for FP) for United States Coast Guard.

1. (U) USNORTHCOM exercises TACON (for FP) for USCG forces that are TACON or OPCON to DoD/USNORTHCOM.

a. (U) USNORTHCOM exercises TACON (for FP) for USCG Law Enforcement Detachments (LEDETs) on Navy ships because USNORTHCOM has TACON (for FP) for the ships.

b. (U) USNORTHCOM retains TACON (for FP) for DoD forces providing support to the USCG.

c. (U) USNORTHCOM does not exercise TACON (for FP) for USCG forces performing normal USCG duties, including when doing so with support from DoD.

(2) (U) Command Headquarters Locations.

(a) (U) USNORTHCOM. Peterson AFB, Colorado Springs, CO.

(b) (U) Headquarters, Department of the Army. Pentagon, Washington, DC.

(c) (U) Headquarters, Department of the Air Force. Pentagon, Washington, DC.

(d) (U) Headquarters, Department of the Navy. Pentagon, Washington, DC.

(e) (U) Headquarters, U.S. Marine Corps. Washington, DC.

(f) (U) JTF-AK. Elmendorf AFB, AK.

(g) (U) JTF-CS. Fort Monroe, VA.

(h) (U) JTF-North. Fort Bliss, TX.

(i) (U) Defense Logistics Agency (DLA). Fort Belvoir, VA.

(j) (U) Defense Threat Reduction Agency (DTRA). Fort Belvoir, VA.

(k) (U) Defense Security Service (DSS). Alexandria, VA.

(l) (U) Defense Commissary Agency (DeCA). Fort Lee, VA.

(m)(U) Defense Contract Management Agency (DCMA). Alexandria, VA.

(n) (U) Defense Intelligence Agency (DIA). Bolling AFB, DC.

(o) (U) National Geo-Spatial Intelligence Agency (NGA). Bethesda, MD.

(p) (U) TRICARE Management Activity (TMA). Falls Church, VA.

(q) (U) Defense Contract Audit Agency (DCAA). Fort Belvoir, VA.

(r) (U) Defense Human Resources Activity (DHRA). Arlington, VA.

(s) (U) Defense Finance and Accounting Service (DFAS). Arlington, VA.

(t) (U) DoD Counterintelligence Field Activity (CIFA). Arlington, VA.

(u) (U) Defense Information Systems Agency (DISA). Arlington, VA.

(v) (U) DoD Education Activity (DoDEA). Arlington, VA.

(w) (U) National Security Agency (NSA). Fort Meade, MD.

(x) (U) Army & Air Force Exchange Service (AAFES). Dallas, TX.

(y) (U) Missile Defense Agency (MDA). Arlington, VA.

(z) (U) Pentagon Force Protection Agency (PFPA). Pentagon, Washington, DC.

b. (U) Command, Control, Communications and Computer (C4) Systems.

(1) (U) The AT information architecture will be an evolving process. Hence, AT information procedures will require modification as AT information capabilities improve or change.

(a) (U) Current Systems. DoD Elements will submit AT/FP information to USNORTHCOM primarily via the following five systems:

1. (U) USNORTHCOM J3 Force Protection / Mission Assurance web portal accessible at the following URLs:
SIPRNET: https://www.noradnorthcom.smil.mil/j3/j34/
NIPRNET: https://www.noradnorthcom.mil/j3/j34/

2. (U) USNORTHCOM Operations Center websites:
SIPRNET: https://www.noradnorthcom.smil.mil/j3/Operations/cog/
NIPRNET: https://www.noradnorthcom.mil/j3/operations/cog/

3. (U) Joint Protection Enterprise Network (JPEN). JPEN is a critical information sharing system and supports essential, reliable, and assured information exchange of Threat and Local Observation Notice (TALON) data, between DoD Elements, enabling decision superiority, battlespace awareness, knowledge, and information management capabilities. JPEN is for the dissemination of TALON and other related FP incident information from the collecting unit to other possibly threatened locations, units, activities or agencies as well as other organizations including analytical centers, such as the Counterintelligence Field Activity (CIFA). JPEN is being fielded to all DoD installations January through June 2005. There is no requirement to purchase hardware or software due to the web-based architecture via the Internet. JPEN Version 2.0 is accessible via any existing NIPRNet or Internet-

capable computer running Internet Explorer 5.5 or higher, and became available at https://www.jpen.mil on 1 Oct 04.

4. (U) Area Security Operations Command and Control system (ASOCC). The ASOCC system is an interactive computer-based system designed to provide situational awareness and collaborative planning capabilities for both military and civilian environments.

5. (U) CORNERSTONE. CIFA is responsible for managing the CORNERSTONE database, which has the ability to create, disseminate, and be the repository for DoD TALON reports. CIFA receives these TALON reports from the Services and makes the determination whether to release information about U.S. persons to analysts. CORNERSTONE is scheduled to be fully automated in the 3rd Quarter of FY05.

(b) (U) Additional systems used by USNORTHCOM to maintain and disseminate AT information include, but are not limited to:

1. (U) Unclassified but Sensitive Internet Protocol Router Network (NIPRNet).

2. (U) Secret Internet Protocol Router Network (SIPRNet).

3. (U) Joint Worldwide Intelligence Communications System. (JWICS)/NORAD/USNORTHCOM Intelligence Systems (NUIS). Network designed to meet the requirements for secure (TS/SCI) multi-media intelligence communications worldwide. JWICS is the SCI component of the Defense Information System Network (DISN). It provides DoD Intelligence Information System (DoDIIS) users a SCI level high-speed multimedia network using high-capacity communications to handle data, voice, imagery and graphics. The system uses JDISS as its primary means of operator interface and display.

4. (U) Community On-Line Intelligence System for End-Users and Managers (COLISEUM): COLISEUM is a DIA automated production and requirements management system. It provides the mechanism for registering and validating requirements; de-confliction of requirements, assignment and scheduling of production; and the capability to track and manage overall production activities across operational and national planners and consumers. COLISEUM is designed to function with the Joint Deployable Intelligence Support System (JDISS) through JDISS/JWICS communications, to other intelligence applications and databases

5. (U) Secure phone communications.

6. (U) Antiterrorism Enterprise Portal (ATEP).

7. (U) Core Vulnerability Assessment Management Program (CVAMP) is located inside the ATEP portal.

8. (U) CIP databases (Joint Staff and the U.S. Marines Corps each have one).

9. (U) Defense Messaging System (DMS) Automated Message Handling System (AMHS) Profiler.

10. (U) New N/NC-J8 automated Planning, Programming, Budgeting, and Execution process (PPBE).

11. (U) Joint Regional Information Exchange System (JRIES). Joint Regional Information Exchange System (JRIES): The DHS established JRIES, a counterterrorism system linking 50 states, five territories, Washington, D.C. and 50 other major urban areas to strengthen its two-way flow of threat information. This system delivers real-time interactive connectivity among state and local partners and with the DHS Homeland Security Operations Center (HSOC). Participants include state National Guard offices, Emergency Operations Centers and first responder and Public Safety departments.

12. (U) INTELINK. Intelink is both an architectural framework and an integrated intelligence dissemination tool for users. The Intelink intelligence network links information in the various classified databases of the U.S. intelligence agencies (e.g., FBI, CIA, Drug Enforcement Administration [DEA], NSA, U.S. Secret Service [USSS] and NRO) to facilitate communications and the sharing of documents and other resources. This system has become institutionalized on the classified networks (SIPRNET and JWICS, formerly Defense Secure Networks [DSNET] 1 and 3) collaboration service providing uniform methods for exchanging intelligence among intelligence providers. Intelink components include:

a. (U) Intelink-U (formerly known as the Open Source Information System [OSIS]).

b. (U) Intelink-SCI.

c. (U) Intelink-P.

d. (U) Intelink-C.

e. (U) Intelink-S, the Secret-level variant of Intelink, has begun to expand rapidly in scope and reach. As the intelligence support medium for GCCS and law enforcement activities, Intelink-S is expected to become the principal growth area for intelligence products and services. Its customer base will be extraordinarily diverse, eventually encompassing all areas of U.S. Government operations that can benefit from integrated intelligence support and collaboration.

13. (U) National Law Enforcement Telecommunications System (NLETS).

14. (U) Global Command and Control System (GCCS).

15. (U) Digital Trunked Radio Systems within the NCR.

16. (U) Geographic Information Systems (GIS).

17. (U) USNORTHCOM Homeland Defense Common Operating Picture (COP).

OFFICIAL:

// SIGNED//
RICHARD J. ROWE, JR.
Brigadier General (P), USA
Director of Operations

// SIGNED//
TIMOTHY J. KEATING
Admiral, USN
Commander, U.S. Northern Command

Annexes:
A Task Organization (U)
B Intelligence (U) - TBP
C Operations (U)
D Logistics. (Omitted)
E Personnel. (Omitted)
F Public Affairs (U)
G Civil Affairs. (Omitted)
H Meteorological and Oceanographic Operations. (Omitted)
J Command Relationships. (Omitted – See paragraph 5.a.(1))
K Command, Control, Communications, and Computer Systems. (Omitted – See paragraph 5.b.)
L Environmental Considerations. (Omitted)
M Geospatial Information and Services. (Omitted)
N Space Operations. (Omitted)
P Host-Nation Support. (Omitted)
Q Health Services. (Omitted)
R Reports
S Special Technical Operations. (Omitted)
T Consequence Management. (Omitted – See NC Plan ___)

U Notional CP Decision Guide. (Omitted)
V Interagency Coordination. (Omitted)
X Execution Checklist. (Omitted)
Z Distribution

ANNEX A TO USNORTHCOM OPORD 05-01 (U)
TASK ORGANIZATION (U)

(U) References: *Base Order*.

1. (U) Situation. Commander, USNORTHCOM exercises TACON (for FP) for all DoD Elements and personnel within the USNORTHCOM AOR. USNORTHCOM AT responsibilities will be executed through the respective DoD Element's AT Program offices.

a. (U) The organizations listed in this Annex are directly subordinate to USNORTHCOM for execution of its FP mission and AT Program.

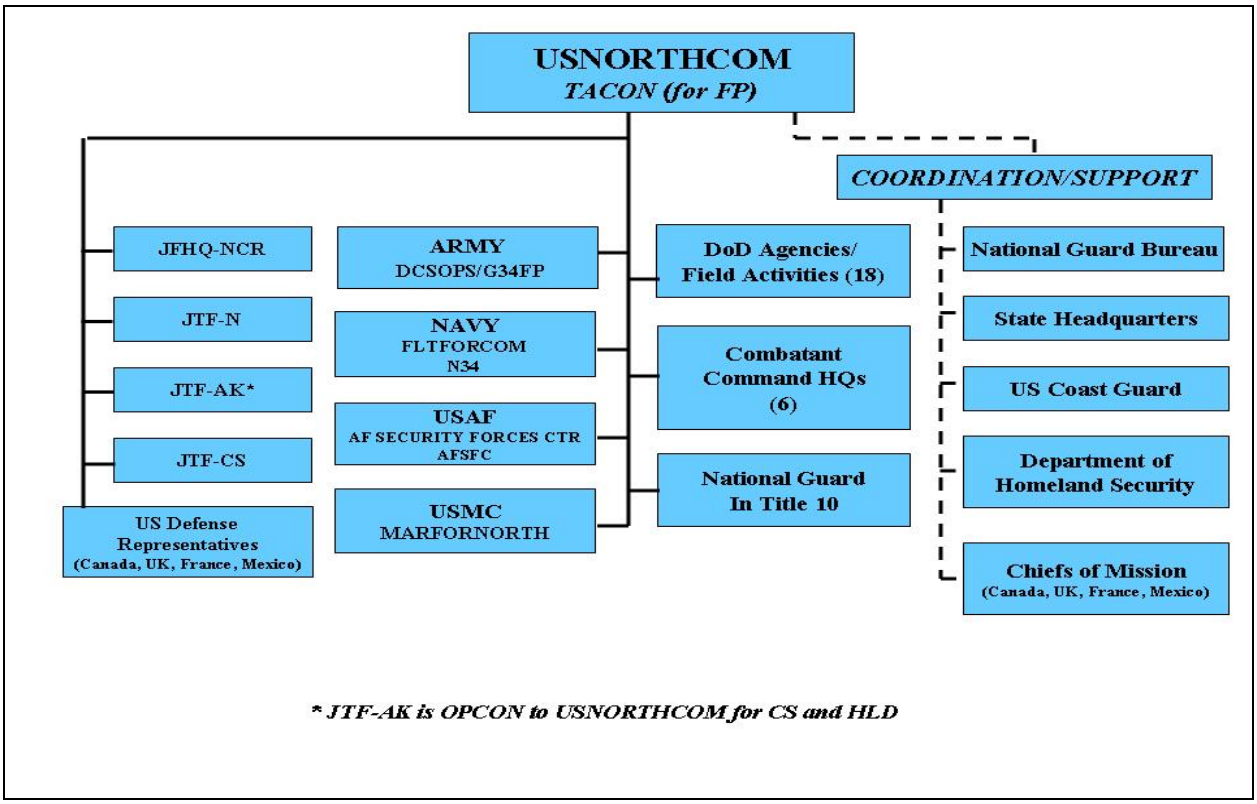


Figure A-1

2. (U) Supporting Geographic Combatant Commands.

ORGANIZATION	COMMANDER
U.S. Pacific Command (USPACOM)	CDRUSPACOM
U.S. Southern Command (USSOUTHCOM)	CDRUSSOUTHCOM

3. (U) Supporting Functional Combatant Commands.

ORGANIZATION	COMMANDER
U.S. Special Operations Command (USSOCOM)	CDRUSSOCOM
U.S. Joint Forces Command (USJFCOM)	CDRUSJFCOM
U.S. Transportation Command (USTRANSCOM)	CDRUSTRANSCOM
U.S. Strategic Command (USSTRATCOM)	CDRUSSTRATCOM

4. (U) Supporting Service Commanders*****.

ORGANIZATION	COMMANDER
U.S. Army Forces Command	CDR FORSCOM
U.S. Navy Fleet Forces Command (FLTFORCOM)	CDR FLTFORCOM
U.S. Marine Forces North (MARFORNORTH)	CDR MARFORNORTH
U.S. Air Combat Command	CDR ACC

***** *Table III-1 (page III-3), note 6 of the Forces For states, "As indicated in the table, a component commander may only be assigned (COCOM) to one combatant commander. A component commander may also provide service to more than one combatant commander through support relationships, as established in this table, under the limitations set forth in the Forces For document."*

5. (U) Supporting Subordinate Commands.

ORGANIZATION	COMMANDER
Joint Force Headquarters – National Capital Region (JFHQ-NCR)	CDR JFHQ-NCR
Joint Task Force – Civil Support (JTF-CS)	CDR JTF-CS
Joint Task Force – North (JTF-N)	CDR JTF-N
Joint Task Force – Alaska (JTF-AK)	CDR JTF-AK

6. (U) Supporting Defense Agencies and DoD Field Activities.

ORGANIZATION	DIRECTOR
Pentagon Force Protection Agency (PFPA)	DIR PFPA
Defense Logistics Agency (DLA)	DIR DLA
Defense Threat Reduction Agency (DTRA)	DIR DTRA
Defense Security Service (DSS)	DIR DSS
Defense Commissary Agency (DeCA)	DIR DeCA
Defense Contract Management Agency (DCMA)	DIR DCMA
Defense Intelligence Agency (DIA)	DIR DIA
National Geo-Spatial Intelligence Agency (NGA)	DIR NGA
TRICARE Management Activity (TMA)	DIR TMA
Defense Contract Audit Agency (DCAA)	DIR DCAA
Defense Human Resources Activity (DHRA)	DIR DHRA
Defense Finance and Accounting Service (DFAS)	DIR DFAS
DoD Counterintelligence Field Activity (CIFA)	DIR CIFA
Defense Information Systems Agency (DISA)	DIR DISA
DoD Education Activity (DoDEA)	DIR DoDEA
National Security Agency (NSA)	DIR NSA
Army & Air Force Exchange Service (AAFES)	DIR AAFES
Missile Defense Agency (MDA)	DIR MDA

7. (U) Task Organization Planning.

a. (U) Joint Task Force – Alaska (JTF-AK). JTF-AK is responsible as a USNORTHCOM Supporting Subordinate Command to execute Commander, USNORTHCOM's FP responsibilities and AT Program in their Geographic Combatant

Commander-designated JOA. In coordination with other military and civil authorities, JTF-AK will protect domestic lines of communication and designated critical infrastructure, essential to the projection of U.S. combat power, within the assigned JOA, in order to protect the U.S. and maintain the nation's freedom of action. Because USPACOM forces are based within the Alaska JOA, JTF-AK is authorized to coordinate directly with USPACOM, as necessary. See Tasks and Responsibilities from this OPORD.

b. (U) USNORTHCOM will coordinate AT Program/FP actions directly with 18 of 27 Defense Agencies and DoD Field Activities (*paragraph 6*.)

c. (U) The Combatant Commands that have headquarters and/or have forces stationed or operating in USNORTHCOM AOR are TACON (for FP) to Commander, USNORTHCOM. The relationship with USPACOM varies from other Combatant Commands, as HQs USPACOM is not within the USNORTHCOM AOR; however, USPACOM has forces that are based within the USNORTHCOM AOR.

d. (U) DoD Elements and personnel that are mobilized or deployed in support of a designated mission where USNORTHCOM is the supported command are TACON (for FP) to Commander, USNORTHCOM. USNORTHCOM FP responsibilities will be executed through the Standing Joint Force Headquarters or command element responsible for the mission in coordination with the Services.

e. (U) The U.S. Defense Representatives (USDR) will coordinate AT matters between the Chiefs of Mission (COM) or Regional Security Officers (RSO) and units or elements that are under a COM for AT.

f. (U) Units and elements are specifically categorized in Memoranda of Agreement (MOA) with the COMs in the USNORTHCOM AOR are under the respective COM for AT. These MOAs are found on the USNORTHCOM AT website on the Secret Internet Protocol Router Network (SIPRNet) portal at https://www.noradnorthcom.smil.mil/j3/j34/MOAs/Forms/AllItems.htm.

g. (U) DoD Elements and personnel within the AOR due to exercises, temporary duty (TDY)/temporary additional duty (TAD), or in-transit status, that are not listed in a given MOA, will fall under their higher headquarters or the subordinate command to which they are or have been assigned for AT.

h. (U) All country clearances, TDY, TAD and deployment orders will clearly indicate whether USNORTHCOM or the COM is responsible for AT, and indicate local AT contacts at the temporary duty site.

ANNEX B TO USNORTHCOM OPORD 05-01 (U)
INTELLIGENCE (U) (TBP)

( ) References:

ANNEX C TO USNORTHCOM OPORD 05-01 (U)
OPERATIONS (U)

(U) References. *Base Order*.

1. (U) General.

a. (U) Purpose. To provide policy, guidance, and to outline the operational requirements, procedures and standards for the USNORTHCOM AT Program.

b. (U) Mission. *Base Order*.

c. (U) Theater. The theater encompassed by this order includes the land, sea, and airspace of USNORTHCOM as defined in the UCP.

2. (U) Concept of Operation.

a. (U) The AT Program fits within the overarching FP mission umbrella. The AT Program is one of several security-related and risk management programs that fall under the overarching FP responsibilities. The AT Program is a collective, proactive effort focused on deterring and mitigating the effects of terrorist attacks against DoD personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism incident management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT Program. The minimum elements of an AT Program are AT risk management, planning, training and exercises, resource generation, and program review.

b. (U) FP Forums. USNORTHCOM will hold and participate in various FP forums to execute and integrate its FP actions and AT Program. The following paragraphs describe these forums in detail.

(1) (U) Force Protection Executive Board (FPEB). This committee is comprised of USNORTHCOM staff directors and special staff principals, as well as General Officer level (or civilian equivalent) representation from each of the Services (4), Combatant Commands (6), assigned forces, and Defense Agencies/DoD Field Activities (18), the National Guard Bureau (NGB), and the United States Defense Representatives (USDR) for Mexico, Canada, France and the United Kingdom. The U.S. Coast Guard is invited to participate in the FPEB. The FPEB is chaired by the Commanding General or the Deputy Commanding General. The committee's composition provides Commander, USNORTHCOM a multi-disciplined forum for ensuring the security, safety, and protection of DoD personnel and facilities throughout the USNORTHCOM AOR. The FPEB provides senior oversight for USNORTHCOM FP actions within the command. The committee is the highest authoritative body responsible to Commander,

USNORTHCOM for addressing FP actions and recommending COAs for theater-wide FP actions. The FPEB meets quarterly, or as required.

(2) (U) USNORTHCOM Force Protection Coordination Committee (NC-FPCC). This committee is comprised of the senior operations officers from each of the Services (4), Combatant Commands (6), assigned forces, and Defense Agencies/DoD Field Activities (18), the Army and Air National Guard, and the USDRs for Mexico, Canada, France and the United Kingdom. The U.S. Coast Guard is invited to participate in the NC-FPCC. The USNORTHCOM J3 will chair the NC-FPCC. This committee will meet at least quarterly to discuss FP policy, plans, training exercises, responsibilities, command and control, and any current or future FP related issues. The purpose of these meetings will be to ensure that USNORTHCOM AT Program issues are coordinated and gain visibility above the Action Officer level. Meetings will be held in the NCR or via Video Tele-Conference (VTC) to reduce TDY/TAD costs. The NC-FPCC serves the same function for USNORTHCOM, as does the DoD FPCC for the Department of Defense. USNORTHCOM is the sponsoring agency and NC/J34 is the Office of Primary Responsibility (OPR) for the NC-FPCC.

(3) (U) USNORTHCOM Force Protection Action Officer (FPAO) Meeting. This committee is comprised of the principal AT representatives from each of the Services (4), Combatant Commands (6), assigned forces, and Defense Agencies/DoD Field Activities (18), the Army and Air National Guard, and the USDRs for Mexico, Canada, France and the United Kingdom. The USNORTHCOM J34 will chair the FPAO Meeting. This committee will meet monthly to discuss FP policy, plans, training exercises, responsibilities, command and control, and any current or future FP related issues. The purpose of these meetings will be to ensure that the USNORTHCOM AT Program is coordinated while identifying and resolving issues. Meetings will be held in the NCR or via Video Tele-Conference (VTC) to reduce TDY/TAD costs. USNORTHCOM is the sponsoring agency and NC/J34 is the Office of Primary Responsibility (OPR) for the FPAO Meeting.

(4) (U) Threat Working Group (TWG). The TWG is a threat or event-driven forum that stands up as the FP crisis action group within the USNORTHCOM Staff. The TWG will consist of O-5 or above (or civilian equivalent) representatives who are cognizant of threats and courses of action (COA) relative to their specific directorates. TWG core membership will specifically include the following personnel or their designated representative: NC/J34 (serves as Chairperson of the TWG), Law Enforcement Senior Advisor, Commander of the Combined Intelligence and Fusion Center (CIFC), Counter Intelligence Staff Officer (CISO), Interagency Coordination (IC) Directorate, Law Enforcement and Security Directorate, USNORTHCOM LS, NC/J33, Current Operations, NC/J35, Future Operations, N-NC/J4, and Command Surgeon. NORAD J3 and J5 also provide personnel. When time permits, representatives from the Services, Unified Commands, the DoD Agencies/Field Activities, and USNORTHCOM assigned units will participate in USNORTHCOM TWGs via VTC or Defense Collaborative Tool Suite (DCTS). The TWG is responsible for reviewing current and potential threats affecting USNORTHCOM operations, personnel, and

resources then providing COAs to include recommendations to Commander, USNORTHCOM for establishment of FPCON for CONUS and OCONUS in order to mitigate and counter the threat. The TWG will assess all-source intelligence, counterintelligence, information operations, force protection, law enforcement, and interagency information to provide a comprehensive threat picture with respect to the USNORTHCOM AOR and operations. The TWG will meet when directed by the Director of Operations, NC/J3 or as requested by any core member of the TWG in order to address emergent or emergency situations that affect operations, personnel, facilities or policy within the USNORTHCOM AOR.

3. (U) Conduct of Operations.

a. (U) Annex C, Operations provides USNORTHCOM direction/guidance on the ten critical tasks delineated in the base order. The crosswalk between the AT Program elements and the ten critical tasks is shown in Figure C-1. These ten critical tasks are inherent within the five AT Program elements and in many cases the execution of a particular task has bearing on multiple elements. The integration of the ten tasks within the five program elements is briefly described below and further in Appendices 1-10. Rules of Engagement (RoE) and Information Operations (IO) are addressed in Appendices 11 and 12 respectively.

AT Program Elements / NC Critical AT Tasks	Information/ Intelligence Flow	AT Policy, Standards & Training Requirement	AT Exercise Program	In-Transit Security & Force Tracking	Implement Security Requirements & FPCON Setting System	AT Vulnerability & Program Assessments	AT Resourcing	Logistics Support for AT	CBRNE Installation Preparedness	Critical Infrastructure Protection
AT Risk Management	X	X		X	X	X	X	X	X	X
AT Planning	X	X	X	X	X	X	X	X	X	X
AT Training and Exercises	X	X	X	X		X			X	X
AT Resource Generation	X	X	X	X	X	X	X	X	X	X
AT Program Assessment	X	X	X	X	X	X	X	X	X	X

Figure C-1

b. (U) Tasks.

(1) (U) Information/Intelligence Flow. This critical task is to ensure systems are in place for timely flow of information/intelligence between USNORTHCOM and DoD Elements in the USNORTHCOM AOR. USNORTHCOM has delineated basic systems (NIPRNet, SIPRNet, DMS, STU/STEAD) and processes for intelligence

assessment/dissemination, suspicious activity reporting, and information sharing on a routine and crisis basis. USNORTHCOM will continue to work with DoD Elements to define and implement systems and processes to maximize intelligence/information flow. (*Annex C, Appendix 1*)

(2) (U) AT Policy, Standards, and Training Requirements. The critical requirement for USNORTHCOM and the DoD Elements in the USNORTHCOM AOR is to establish the appropriate processes for coordination to ensure appropriate standardization and unity of effort, resulting in a coherent, seamless defensive posture in the USNORTHCOM AOR. (*Annex C, Appendix 2*)

(3) (U) AT Exercise Program. The requirements for AT training and exercises are articulated in DoDI 2000.16, standard 19. This critical task specifically addresses the DoDI 2000.16 standard as well as specific USNORTHCOM requirements. (*Annex C, Appendix 3*)

(4) (U) In-Transit Security and Force Tracking. This has been designated as a critical task for USNORTHCOM because the AT responsibilities associated with execution of this task cross Service boundaries, Unified Command boundaries, and requires coordination with critical infrastructure protection (CIP) and other key components of the FP construct, as well as the Department of Homeland Security (DHS) for interface with civilian agencies. (*Annex C, Appendix 4*)

(5) (U) Implement Security Requirements and FPCON Setting System. This critical task addresses the requirement to establish processes for the development and implementation of additional security measures that may exceed the parameters of the FPCON system based on specific mission requirements. These processes will be established to ensure coordination and consistency in security related decisions for the USNORTHCOM AOR. Additionally, FPCON setting and the processes for coordination are critical for USNORTHCOM and the DoD Elements in the USNORTHCOM AOR. As the primary responsibility to establish the baseline, it is critical that the Commander, USNORTHCOM has the right information to make an informed decision. Execution of this task has a significant impact on the operational missions of DoD Elements in the USNORTHCOM AOR and JOAs. (*Annex C, Appendix 5*)

(6) (U) AT Vulnerability and Program Assessments. The Vulnerability Assessment (VA) process and resulting database provide a common operational picture for the USNORTHCOM AOR. For USNORTHCOM, the VA database is the centerpiece for assessing the security posture of the USNORTHCOM AOR. The AT VA program, when integrated with the CIP and IO VA programs, will provide a comprehensive picture. When the VA programs are synchronized with current intelligence/information, it will facilitate timely and accurate decisions regarding FP. (*Annex C, Appendix 6*)

(7) (U) AT Resourcing. This critical task is derived from USNORTHCOM's responsibility as an advocate for the DoD Elements' AT requirements in the PPBE

process and to manage the CbT RIF program for the USNORTHCOM AOR. (*Annex C, Appendix 7*)

(8) (U) Logistics Support for AT. Although the DoD Elements are responsible for contracting and construction programs under Title 10, compliance with AT guidelines and instruction is critical to prevent and/or mitigate against potential terrorist attacks. This appendix covers processes for USNORTHCOM to validate that AT requirements are being met under established Service and Defense Agency/DoD Field Activity construction and contracting programs. (*Annex C, Appendix 8*)

(9) (U) CBRNE Installation Preparedness. The responsibility to integrate CBRNE training, exercises, and plans into overarching installation AT plans is critical for synchronized operations. USNORTHCOM's responsibility is to establish the processes to ensure policy and plans are developed that focus installation CBRNE preparedness, to include interface with local civilian communities. This is critical not only for FP actions but for incident management (which includes crisis response and consequence management) as well. (*Annex C, Appendix 9*)

(10) (U) Critical Infrastructure Protection. The responsibility to integrate CIP training, exercises, and plans into overarching installation AT plans is critical for synchronized operations. USNORTHCOM's responsibility is to establish the processes to ensure policy and plans are developed that focus on protecting or mitigating the effects to infrastructure critical to mission accomplishment. (*Annex C, Appendix 10*)

Appendices:
1 Information/Intelligence Flow (U)
2 AT Policy, Standards, and Training Requirements (U)
3 Develop an AT Exercise Program (U)
4 In-Transit Security and Force Tracking (U)
5 Implement Security Requirements and FPCON (U)
6 AT Vulnerability and Program Assessments (U)
7 AT Resourcing (U)
8 Logistics Support for AT (U)
9 CBRNE Installation Preparedness (U)
10 Critical Infrastructure Protection (U)
11. Rules of Engagement (U)
12. Information Operations (U) – To Be Published
13. Force Health Protection (U)
14. Sample AT Plan Format (U)
15. Sample Risk Assessment (U)
16. USNORTHCOM Staff Tasks (U)

APPENDIX 1 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
INFORMATION/INTELLIGENCE FLOW (U)

(U) References: *Base Order*.

a. (U) CJCSM 3150.03B, Joint Reporting Structure Event and Incident Reports, July 28 2003.

1. (U) Situation. *Base Order*.

2. (U) Mission. *Base Order*.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) This critical task is to ensure systems are in place and operational to support the timely flow of information/intelligence between USNORTHCOM and the Combatant Commands, Services, Defense Agencies and DoD Field Activities operating in the USNORTHCOM AOR. The establishment of processes directly facilitates the exchange of threat, crisis and routine information or intelligence. This task is derived from DoDI 2000.16 standards 7-9, 15, 26, and 27 as well as DoDD 2000.12 requirements 5.14.1, 5.14.3, 5.15.1, 5.15.6, and 5.17.1 through 5.17.18.

(2) (U) The NC/J34 provides continuous coordination within and outside the command to synchronize the information/intelligence flow concept, identify requirements and responsibilities, and develop operational procedures. The resultant effort establishes the reporting and information sharing processes to facilitate situational awareness across the USNORTHCOM AOR and to effectively plan and execute the AT Program. This appendix outlines the information architecture or systems; identifies the criteria subject to threat, crisis, and routine information/intelligence reporting or sharing; and outlines the processes to facilitate the exchange.

(3) (U) AT Information Architecture/Systems. To facilitate information flow critical to maintain situational awareness and create the common operational picture desired by USNORTHCOM required additional systems be established. Additional systems were not created to minimize the use of current systems, such as, DSN, SIPR/NIPR email, VTC, DMS, JWICS, JRIES, and numerous others. The use of all systems will not be discussed as most are used in the normal conduct of daily operations. Described herein are specific systems designed to provide the interface between the DoD Elements and USNORTHCOM. These systems are all in the fielding and employment phase.

(a) (U) USNORTHCOM J3 Force Protection / Mission Assurance (FP/MA) Web-Based Portal. Management of the NC-J3 FP/MA web portal page is the responsibility of the NC-J34. The web-based portal pages were adopted for use based

on the need to match current technology and systems in use at the lowest level for all DoD Elements. The website is designed to facilitate information sharing, enhance situational awareness, and serve as the foundation for maintaining a common operating picture. It is designed to facilitate user capability to push or pull information. The website is the repository for all FP-specific information to include AT, CIP, CBRNE, assessments, SITREPs, and FPCONs. While created on both the NIPRNet and SIPRNet, the ultimate goal is for the majority of use to be on the classified network. The website is divided into two distinct areas: homepage and restricted access.

1. (U) NC/J34 Homepage (FP/MA). The homepage is populated with numerous documents, links, and announcements. It provides information on FPCON updates, FP messages and advisories, FP Working Groups, Threat Working Groups, FP Executive Boards, Theater Clearance/Force Tracking, AT links, publications, and other relevant FP topics. This page may be accessed from any .gov or .mil computer network. The URLs are identified below.

a. (U) SIPRNet URL: https://www.noradnorthcom.smil.mil/j3/j34/

b. (U) NIPRNet URL: https://www.noradnorthcom.mil/j3/j34/

2. (U) NC/J34 (FP/MA) Restricted Access Portal. This sub-web is designed to be the venue to pass Law Enforcement (LE) sensitive information, vulnerability information, and other limited distribution information to authorized persons. It will also be used to upload required monthly FP Updates. Access requirements and instructions although fielded in separate correspondence will be posted to the homepage.

(b) (U) Joint Protection Enterprise Network (JPEN) and Threat and Local Observation Notice (TALON).

1. (U) JPEN is a critical information sharing system and supports essential, reliable, and assured information exchange of TALON data, between DoD Elements, enabling decision superiority, battlespace awareness, knowledge, and information management capabilities. JPEN is designed for the dissemination of TALON and other FP incident information from the collecting unit to other possibly threatened locations, units, activities or agencies as well as other organizations including analytical centers, such as CIFA. JPEN is being fielded to all DoD installations January through June 2005. There is no requirement for either “fielding” hardware or software to specific installations due to the web-based architecture via the Internet. JPEN Version 2.0 is accessible via any existing NIPRNet or Internet-capable computer running Internet Explorer 5.5 (or higher), and became available at https://www.jpen.mil on 1 Oct 04. The concept of employment outlining fielding information, account registration and user training plans is posted on the USNORTHCOM NC/J34 website.

2. (U) TALON reports were established to provide a means to capture non-validated domestic threat information, create a standardized reporting format adaptable to analysis, and incorporate it in the DoD terrorism threat warning process as appropriate. A TALON report consists of raw information regarding suspicious incidents and must be entered into JPEN. Information in TALON reports is non-validated (may or may not be related to an actual threat) and by its very nature may be fragmented and incomplete. The purpose of the TALON report is to document and immediately disseminate potential threat information to DoD personnel, facilities, and resources. The TALON mechanism is not designed to take the place of the formal intelligence reporting process. All DoD intelligence, counterintelligence, LE, and security organizations that have the mission to collect FP and threat information will identify, collect, and report the following categories of information, in accordance with existing policy and Deputy Secretary of Defense Memorandum dated 2 May 03:

a. (U) Non-specific threats of DoD interests.

b. (U) Suspected surveillance of DoD facilities and personnel.

c. (U) Elicitation attempts, suspicious questioning, or other suspected intelligence collection activities focused on DoD interests.

d. (U) Tests of security.

e. (U) Unusual repetitive activity.

f. (U) Bomb threats.

g. (U) Any other suspicious activity and incidents reasonably believed to be related to terrorist activity directed against DoD personnel, property, and activities within the United States.

(c) (U) Area Security Operations Command and Control System (ASOCC). The ASOCC system is an interactive computer-based system designed to provide SA and collaborative planning capabilities for both military and civilian environments. Development of the concept of employment outlining future fielding has not been finalized.

b. (U) Tasks.

(1) (U) Reporting and Information Sharing Requirements.

(a) (U) Information/intelligence exchange from all DoD Elements TACON (for FP) to USNORTHCOM will be accomplished in the following manner:

1. (U) As designated by the DoD Elements, operations centers, watches, AT managers or security officers will transmit official message traffic (voice, email,

DMS) or required reports to the USNORTHCOM Operations Center (NCOC), and courtesy copy NC/J34 as appropriate.

2. (U) AT representatives from the DoD Elements have direct liaison authority with NC/J34 on all AT matters to expedite communications.

(b) (U) Routine or crisis information/intelligence exchange from USNORTHCOM to the designated message entry points, after-hours POC, or 24-hour control center of the DoD Elements will be transmitted under the direction and approval of the USNORTHCOM Director of Operations (J3) or designated representatives. This will ensure the timely release of message traffic from either the USNORTHCOM Operations Center (NCOC) or NC/J34 as appropriate.

(c) (U) Contact Information for USNORTHCOM. Contact information for the NCOC, N-NC/J2, NC/J3, NC/J34, and Combined Intelligence Fusion Center (CIFC) is located in Tab A to Appendix 1 to Annex C.

(d) (U) Reports are addressed in *Annex R, Reports*.

(e) (U) Routine Reporting. Routine reporting is defined as information required by Commander, USNORTHCOM, the Director of Operations (J3) and NC/J34 to support day-to-day operations. This information will support standing Commander's Critical Information Requirements (CCIR). Baseline AT reporting requirements will be submitted by all DoD Elements in a Monthly FP Update via the NC/J34 (FP/MA) restricted portal. Monthly FP Updates will be submitted IAW the guidance provided (*Annex R, Reports*).

(f) (U) Event-Dependent Reporting. Information required by Commander, USNORTHCOM to support situational dependent events will be submitted IAW the following requirements and procedures. Deployed or mobilized forces supporting HLD, CS or other missions where Commander, USNORTHCOM is the supported commander are required to include FP information in the appropriate paragraph of their commands situation report. In addition, events that dictate DoD Elements raise their FPCON baseline or deviate below established baselines are reportable. Event-dependent reporting requirements are amplified below.

1. (U) Deployed/Mobilized Force or Supporting Commander FP paragraph of the USNORTHCOM SITREP. Deployed/mobilized forces in support of USNORTHCOM will provide a minimum of the following information:

a. (U) Current FPCON condition with measures from higher FPCONs.

b. (U) Identify vulnerabilities in priority that cannot be mitigated and requires assistance.

c. (U) Projected future actions.

d. (U) Commanders evaluation/assessment.

2. (FOUO) FPCON Change Reports. FPCON change reports are required to be transmitted to the NCOC through the DoD Elements' chains of command within four (4) hours of implementing the change. FPCON Change Reports apply to all changes elevating an FPCON or changes decreasing an elevated FPCON. Reports should be rendered utilizing OPREP-3 reporting format and procedures IAW *ref. a* to the NCOC and copied to the NC/J34. This includes initial voice notification and record copy (message) reports. Upon submittal and HHQ acknowledgement of these reporting actions, FPCON status change shall also be updated in JPEN and/or ASOCC.

a. (FOUO) General Instructions.

1) (U) USNORTHCOM FPCON change reporting applies to DoD FPCON and Homeland Security Advisory System Alert Activity Level (or referred to as GSA Threat Advisory System) that any DoD Element may be subject to.

2) (U) Any DoD Agency with a facility/activity/office/etc. regulated by Homeland Security Advisory System (HSAS) Alert Activity Levels will use the Homeland Security Advisory System as the baseline to determine reporting applicability.

3) (FOUO) FPCON change reports apply to any size installation/activity/location within the DoD Elements. This includes depots, maintenance facilities, office buildings, off-installation activities, recruiting stations, etc. Size is not reflective of the number of personnel residing on or working in a DoD-controlled/leased/owned space nor is it based on square footage or physical space occupied.

4) (FOUO) FPCON change reports are not required for separate units/activities that are tenants of other DoD facilities/installations who have a FPCON reporting requirement to USNORTHCOM. (e.g. For USMC Det. 639 based on Andrews AFB, FPCON changes for Andrews and those that may affect Det. 639 are reported by the USAF.)

5) (FOUO) FPCON change reports are submitted for separate units/activities that are tenants of other facilities/installations (GSA leased space, etc.) who do not have a FPCON reporting requirement to USNORTHCOM. (e.g. Office space occupied by DCAA in a building that follows DHS Alert Levels would be reported by DCAA).

b. (FOUO) Report Applicability.

1) (FOUO) Change of the Service/Combatant Command/DoD Agency/Field Activity FPCON baseline within the USNORTHCOM AOR.

2) (FOUO) Change of any DoD Element subordinates (installation, activity, location, facility, office building, etc.) FPCON that are a full level above their commands FPCON baseline directives (not USNORTHCOM's).

3) (FOUO) Change of any DoD Element subordinates (installation, activity, location, facility, office building, etc.) FPCON that are deviating from their commands FPCON baseline directives and are at a full level below that of the USNORTHCOM FPCON baseline.

4) (FOUO) Any Defense Agency/DoD Field Activity whose facilities/activities/offices are under the control and jurisdiction of non-DoD Federal agencies, specifically GSA non-delegated facilities, report changes that are above or below the HSAS level.

c. (FOUO) Report Content.

1) (FOUO) Affected DoD Element: State who is affected. (Army; Peterson AFB, CO; Defense Depot Susquehanna, PA; DCAA office, St Louis, MO; etc).

2) (FOUO) New FPCON Level: State FPCON level with any higher level measures. (FPCON ALPHA with B3, B5-7, C4).

3) (FOUO) DTG Effective: State date and time the new FPCON was implemented or went into effect. (100450Z JAN 05).

4) (FOUO) Why: State why or what caused the change. Brief but detailed description of why/what.

5) (FOUO) Who Directed: State who directed the change. (Army Chief of Staff; DCAA Director; Installation Commander; etc)

6) (FOUO) Duration of Change: State the duration or anticipated duration. (Effective upon receipt and until further notice; effective through the New Year and ending 5 Jan 05; pending outcome of threat/vulnerability assessment; etc).

(g) (U) Suspicious Activity or Threat Reporting. Time sensitive CI, suspicious activity or threat reports that identify vulnerabilities and/or threats to a specific unit, command, or location will be immediately forwarded to the affected command by USNORTHCOM. A DoD Element having information of this type should notify NCOC as rapidly as possible. *Ref. a* provides the guidance and procedures for OPREP messaging for all DoD Elements. After initial reporting has been made, all other related information/intelligence notification will be made through routine channels.

1. (U) Suspicious Activity/TALON Reports. In general, most TALON reporting will be executed through JPEN as described in paragraph 3.a.(3)(b). However, any command identifying criteria stated in the preceding paragraph should

notify USNORTHCOM of its posting to JPEN and not assume the report has been viewed.

2. (U) Time Sensitive Counterintelligence (CI) or Intelligence Reports. Information believed to meet BLUE DART threat-warning reporting criteria must be reported by any unit that receives such information through its respective organizational structure. This information will be sent via OPREP-3 reporting procedures with an IMMEDIATE or FLASH precedence to the NCOC. Voice reports must reach USNORTHCOM within one hour of the reporting unit's initial report. A record copy report must reach USNORTHCOM within two hours of the reporting unit's initial report. USNORTHCOM will disseminate information of this nature not meeting the release of a threat-warning message to provide situational awareness and will do so IAW OPREP-3 procedures.

3. (U) Threat Warning Reports. The BLUE DART is an AT threat-warning program designed to rapidly disseminate threat information directly to affected areas and units in a simple, easy to understand format. Amplification of the BLUE DART program is located in Tab B to Appendix 1 to Annex C.

(h) (U) Crisis Reporting. The primary emphasis of crisis reporting is focused on suspected or confirmed terrorist incidents that have affected or potentially affect the operations, facilities or personnel of the DoD Elements. Notification throughout the chain of command, to all DoD Elements and the National Military Command Center (NMCC) will be accomplished utilizing OPREP-3 Pinnacle reporting procedures and timelines.

1. (U) Once either a suspected incident or confirmed incident has occurred ensure the rapid notification of all personnel assigned. These actions are necessary to ensure a heightened state of alert has been obtained to prevent attacks or deter possible subsequent attacks and to facilitate the control of the attack that just occurred.

2. (U) Initial notification should include at a minimum the following information. However, do not delay the initial report to gain additional information.

a. (U) Date, Time, and Location of incident.

b. (U) Type of incident such as bombing, kidnapping, or direct assault.

c. (U) Number of casualties (as known or estimated).

d. (U) Summary of current security status.

3. (U) The follow-up message to the initial notification should provide the necessary information to generate an OPREP-3, and should include at minimum the following information:

a. (U) Information on the current situation, status of treatment for casualties: numbers, not names.

b. (U) Accountability for all personnel. Report total personnel by category aboard the ship or on the installation by unit. For example, a report could include all personnel by Service Officer/Enlisted/Civilian, then all other Government civilians, followed by contractors.

c. (U) A concise description of the incident that clearly states if this was a terrorist incident, an accident, or a simple crime against persons. In any case, state the disposition of the search and capture of the perpetrators by authorized personnel, and the reliability of this information.

d. (U) A statement of the current and future security situation for the installation, unit equipment, and all personnel in the immediate area and under the control of the reporting commander. Include any impact of the current situation on local American citizens.

e. (U) Report the impact of the incident on the ship/unit/installation's ability to accomplish its mission.

f. (U) Actions being taken within the constraints of the commander's current Rules of Engagement (ROE) or Rules on the Use of Force (RUF). Assess the vulnerability of the ship/site, as well as remaining ships/sites and personnel.

g. (U) Forces readily available. Include a list of those forces and equipment needed immediately to augment and reinforce ship/installation/unit personnel to provide critical functions. Provide specifics for each requirement where possible (i.e. how much, how many, when needed, recommended delivery mode, delivery locations, etc.). Forces could include:

1) (U) Medical support.

2) (U) EOD support.

3) (U) Security Forces and Equipment.

4) (U) Search and Rescue Support.

5) (U) Public Affairs.

6) (U) Communications.

7) (U) Legal Support.

8) (U) Translators.

9) (U) Transportation.

10) (U) Chaplain Support.

h. (U) The time for earliest force commitment and the required arrival time for any requested critical forces.

i. (U) Intelligence/Counterintelligence.

(2) (U) Requests for Information (RFI).

(a) (U) RFIs are categorized into two distinct realms: operational and intelligence. Operational requests encompass AT plans, policy, training, operations, assessments, resources, CBRNE and CIP. RFIs of this nature will be processed through NC/J34. Intelligence RFIs, to include law enforcement sensitive, will be processed through the USNORTHCOM CIFC, as appropriate.

1. (U) Operational RFIs.

a. (U) Prior to submitting any RFIs to USNORTHCOM the requesting organization should attempt to acquire the information through its higher command.

b. (U) Operational RFIs may be submitted to NC/J34 organizational mailbox at nc.j34.rm.omb@northcom.smil.mil or nc.j34.rm.omb@northcom.mil.

2. (U) Intelligence RFIs.

a. (U) Primary. The primary means to request intelligence is through the requestor's organizational intelligence office / directorate or its the supporting intelligence office. RFIs that cannot be answered will normally be submitted through the Community On Line Intelligence System for End-Users and Managers (COLISEUM) at http://coliseum-s.dia.smil.mil/. COLISEUM forwards requests to the organization best able to assess the threat and allows other customers to have access to the information provided.

b. (U) Alternate. If an organization does not have access to COLISEUM, RFIs may be forwarded through the next higher intelligence office in the organization's chain of command or through the DoD Element's AT Program Manager to the USNORTHCOM J22 CIFC. The CIFC will provide NC/J34 a copy of all RFIs. Submit RFIs to the one of the following organizational mailboxes: nc.j22a.omb@northcom.smil.mil or nc.cifca.omb@northcom.smil.mil.

3. (U) RFI Requirements. The following information is required when submitting RFIs via email:

a. (U) Subject.

b. (U) Date Desired (DTG).

c. (U) Last Time of Value (DTG).

d. (U) Priority (Routine, Priority, Flash).

e. (U) Classification.

f. (U) RFI Text.

g. (U) Requestor's Name.

h. (U) Requestor's Command.

i. (U) Requestor's Office.

j. (U) Requestor's Email.

k. (U) Requestor's Telephone (Comm/DSN).

Tabs:

A. Contact Information (U)
B. BLUE DART Threat Warning Program (U)

TAB A TO APPENDIX 1 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
CONTACT INFORMATION FOR USNORTHCOM (U)

1. (U) USNORTHCOM Operations Center (NCOC) (24-hour operations):

   Phone: 719–554–2361 (DSN 692–2361)

   Classified email: nc.cog.chief.omb@northcom.smil.mil or nc.cog.dl@northcom.smil.mil

   Unclassified email: nc.cog.chief.omb@northcom.mil or nc.cog.dl@northcom.mil

   DMS: HQ USNORTHCOM PETERSON AFB CO//DWC//

2. (U) USNORTHCOM CIFC:

   Phone: 719–554–8612 (DSN 692–8612)

   Classified email: nc.j22a.omb@northcom.smil.mil or nc.cifca.omb@northcom.smil.mil

   Unclassified email: nc.j22a.omb@northcom.mil or nc.cifca.omb@northcom.mil

   DMS: COMBINED INTEL CTR PETERSON AFB CO//J2A//

3. (U) USNORTHCOM J3:

   Phone: 719–554-4998 (DSN 692-4998)

   Classified email: nc.j3.omb@northcom.smil.mil

   Unclassified email: nc.j3.omb@northcom.mil

   DMS: HQ USNORTHCOM PETERSON AFB CO//J3//

4. (U) NORAD-USNORTHCOM J2:

   Phone: 719–554–5212 (DSN 692–5212)

   Classified email: nc.j2.omb@northcom.smil.mil

   Unclassified email: nc.j2.omb@northcom.mil

   DMS: HQ USNORTHCOM PETERSON AFB CO//J2//

5. (U) USNORTHCOM J34:

Assessments Branch Phone: 719–554–7127/7126/6121 (DSN prefix 692)

Email: SIPR: nc.j34.va.omb@northcom.smil.mil
NIPR: nc.j34.va.omb@northcom.mil

Plans, Policy, Training & Exercises Branch Phone: 719–554–6943/8306/7130

Email: SIPR: nc.j34.ppte.omb@northcomsmil.mil
NIPR: nc.j34.ppte.omb@northcom.mil

Resource Management Branch Phone: 719–554–8308/2375 (DSN prefix 692)

Email: SIPR: nc.j34.resources.omb@northcom.smil.mil
NIPR: nc.j34.resources.omb@northcom.mil

Force Protection Risk Management Branch:

Email: SIPR: nc.j34.rm.omb@northcom.smil.mil
NIPR: nc.j34.rm.omb@northcom.mil

AT Operations Phone: 719–554–8311/3897/8305 (DSN prefix 692)

CBRNE Phone: 719–554–7136/7129/7135 (DSN prefix 692)

CIP Phone: 719–554–7134/2374/2375 (DSN prefix 692)

DMS: HQ USNORTHCOM PETERSON AFB CO//J34//

TAB B TO APPENDIX 1 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
BLUE DART THREAT WARNING PROGRAM (U)

1. (U) General.

a. (U) BLUE DART is an AT threat-warning program designed to disseminate threat information directly to affected areas and units in a simple, easy to understand format. The program covers all DoD Elements TACON (for FP) to USNORTHCOM. Within USNORTHCOM, threats to the Headquarters elements, subordinate commands and forces, and allied units operating under USNORTHCOM auspices (e.g., Canadian units) are subject to BLUE DART reporting requirements. Requirements will not apply to civilian organizations or interests (e.g., commercial airlines), foreign governments, or out-of-AOR U.S. Government facilities. These organizations are subject to other reporting mechanisms. BLUE DART is a Command-wide program, and dissemination of BLUE DART warning messages will not be limited to intelligence channels.

b. (U) A BLUE DART originating in HQs USNORTHCOM may only be executed by the NCOC at the direction of the NC/J3. DoD Elements currently using BLUE DARTs will continue doing so using their established procedures and will copy the NCOC. BLUE DART is a means of disseminating a time-critical threat warning and is issued when a specific set of criteria information has been met. Criteria may be generated from a number of sources to include, intelligence activities supporting USNORTHCOM and other DoD Elements, civilian LE entities or through reporting from installation/activity levels. It must contain all of the following elements:

(1) (U) This information must specify:

(a) (U) TIMING of a threat: specific near-time frame within the next 72 hours.

(b) (U) TARGET of a threat: i.e., exact unit, activity or location.

(c) (U) TYPE or means of a threat: i.e., explosives/VBIED, bombing, small arms/drive by, sniper, and biological attack.

(2) (U) Specificity is the key principle of this program. Threat information containing the three elements above, and determined to be a valid and credible threat by the command intelligence activity, will be disseminated via a BLUE DART message.

c. (U) BLUE DART requires two forms of notification. Immediate voice notification by telephone or radio directly to the targeted unit or installations parent organizational operations or watch center ensures threat information is passed by the fastest means possible. It also allows for authentication by the BLUE DART message recipient with the originator and provides immediate feedback from the receiving unit, thereby confirming its reception and interpretation. Record copy notification is then accomplished through OPREP-3 reporting formats utilizing appropriate message

handling systems. Voice notification must be completed within fifteen minutes of BLUE DART message initiation. Record OPREP-3P message traffic from the BLUE DART originator will follow within one hour of the initial report.

d. (U) The USNORTHCOM J34 (NC/J34) is the overall staff proponent for the BLUE DART program. NC/J34 is responsible for program implementation, exercises, and policy/procedure development.

e. (U) Scope of Program.

(1) (U) BLUE DART applies to real world imminent threat and EXERCISE/WHITE PINNACLE/BLUE DART exercise warnings. The BLUE DART program will be coordinated, deconflicted and exercised through a combined effort of the NCOC and NC/J34.

(2) (U) BLUE DART reports will be given the widest dissemination to ensure commanders have adequate information on which to base guidance and assistance to threatened units, activities or locations.

(3) (U) BLUE DART is meant for time-critical threat warning of a specific nature. Warnings not conveying an imminent threat and identifying a specific unit, ship or location generally should not be disseminated as a BLUE DART unless an incident suggests follow-on threats are likely and imminent. Examples are provided below.

(a) (U) A threat report with a specific threatened unit (10^{th} Ranger Brigade), activity (VA Hospital) or location (Fort Blank); a specific threat type or means (explosive device/suicide bomber); within a specific near-term time frame within the next 72 hours normally would be reported as BLUE DART.

(b) (U) A report of a general threat to troops without location, time frame, or means would not be a BLUE DART.

(c) (U) A report of an individual or isolated incident (explosion, sniper fire) that has already taken place would not normally be reported as a BLUE DART unless it is believed more incidents will follow.

(4) (U) Any unit that receives information believed to meet BLUE DART criteria should immediately report through their respective organizational structure to the NCOC and copy to NC/J34. This information will be sent via OPREP-3 reporting procedures with a FLASH precedence. A voice report must reach USNORTHCOM within one hour of the reporting unit's initial report. A record copy report must reach USNORTHCOM within two hours of the reporting unit's initial report.

2. (U) Execution.

a. (U) Threat Dissemination.

(1) (U) Initial Warning Report. BLUE DART warnings will be passed to the threatened unit, activity or location by the most efficient means possible. Initial notification from USNORTHCOM will be passed to the identified service, combatant command, Defense Agency or DoD Field Activity 24-hour/7-day a week operations center or watch and the NMCC. Non-secure communications may be used but only when secure means are unavailable or judged to be too slow. It is inherent upon all DoD Elements to establish written threat warning dissemination procedures to ensure timely introduction of a BLUE DART threat warning to command and control nets, intelligence centers, and across all echelons of the organization.

(a) (U) Voice Report Format. BLUE DART threat-warning reports will be passed in accordance with the provided format. (*Annex R, Reports*)

(b) (U) The BLUE DART message receiver will conduct a call back to the message originator/sender to authenticate the identity of the sender and verify the information.

(2) (U) Subsequent (Record Copy) Reports. Initial voice notification to the targeted DoD organization will be followed with FLASH precedence, OPREP-3P record message traffic. This message traffic will be submitted at a minimum to the threatened command/OPCEN, all DoD commands and organizational Headquarters, and the NMCC. (*Annex R, Reports*)

(3) (U) BLUE DART Acknowledgment**.** All DoD Elements are required to ensure that USNORTHCOM receives acknowledgement that the threatened unit/activity/location received the threat warning. Acknowledgement report must be rendered within 30 minutes of notification to the threatened unit and will include DTG message received by the threatened unit, who at the threatened unit/activity/location received the BLUE DART message, and method of receipt or communication (how they were notified). Method of transmission back to USNORTHCOM may be through any appropriate message handling system in OPREP-3 format.

b. (U) Dissemination Procedures.

(1) (U) All Services, Combatant Commands, Defense Agencies and DoD Field Activities are responsible for establishing local procedures to disseminate BLUE DART warnings down and across all echelons. This requires all DoD Elements to compile 24-hour contact procedures for each installation or facility supporting personnel or activities and to have checklists in place to facilitate rapid dissemination of BLUE DART messages.

(2) (U) NCOC Notification to the NMCC.

(a) (U) Voice Reports:

1. (U) Primary Telephone: (DSN) 851-3840

2. (U) Secondary Telephone: (DSN) 227-6340; COMM (703)-697-6340

3. (U) Washington Switch: (703) 697-1201 (ask for NMCC connection)

(b) (U) Record Communication Reports. Message Addresses:

1. (U) AUTODIN: JOINT STAFF WASHINGTON DC//J3 NMCC

2. (U) DMS: JOINT STAFF J3 NMCC OPS

c. (U) Protection of Classified Information. Classified threat warning information will be protected to the maximum extent possible consistent with the need to inform threatened units within fifteen (15) minutes of receipt of the initial BLUE DART warning message. Certain sensitive sources of information, if compromised, would be irreplaceable, potentially leading to significant degradation of intelligence to the supported commander. Despite this risk of loss, nothing in this guidance overrides a unit's responsibility to report information critical to the protection and survival of U.S. and allied forces within the USNORTHCOM AOR by the most expedient means possible, though secure means are preferred. Likewise, the nature of the threat identified in a BLUE DART message may be shared with responsible local, State, and Federal law enforcement agencies where DoD Elements and personnel reside in facilities off DoD installations and rely on these agencies for increased security and response capabilities.

d. (U) Redundant Communications. Voice and message dissemination are necessary to ensure timely delivery of imminent threat warning information. All initial BLUE DART voice reports will be followed-up with hard copy (record message, e-mail or fax) message traffic. Send voice reports to follow-up and to confirm receipt of initial reporting when/if BLUE DART is carried out via message, e-mail, or data link. Use broadcast wherever possible to ensure widest dissemination in the shortest time.

e. (U) Operational Intelligence Watch (OIW) Support. The NORAD/USNORTHCOM OIW will immediately notify the NCOC of threat related information meeting or believed to meet BLUE DART criteria. The NCOC assumes BLUE DART message release approval and subsequent dissemination responsibilities within the USNORTHCOM AOR.

3. (U) Administration and Logistics. DoD Elements are responsible to notify Commander, USNORTHCOM via their chains-of-command, of equipment or procedural shortfalls that would prevent execution of provisions of this guidance.

4. (U) Command and Control (C2). All DoD Elements are responsible to establish a BLUE DART Threat Warning program that integrates this guidance and creates a system conducive to rapid threat-warning dissemination. Secure telephone or secure

radio, if available, will be used for immediate voice notification. The record copy report will be sent via hard copy message. With the advancements of data communication technology the initial report may be sent by automated means, but must be followed-up with voice confirmation.

5. (U) EXERCISE/WHITE PINNACLE/BLUE DART Procedures.

a. (U) NCOC and NC/J34 will synchronize and implement EXERCISE/WHITE PINNACLE/BLUE DART procedures, at a minimum, once a quarter to maintain program awareness and message dissemination proficiency. Exercise messages will be sent only with the approval of NC/J3, and only after appropriate staff coordination has been completed. Test considerations are as follows:

(1) (U) Exercise messages will test the voice notification system and utilize the voice report format provided in paragraph 5.e.(1). Record message traffic will be passed IAW the format provided in paragraph 5.e.(2). Exercise message formats and procedures will mirror real-world messages as close as feasible.

(2) (U) Exercise message implementation is intended to involve a variety of units/activities/locations to ensure circuits and procedures function properly.

(3) (U) Exercise messages will not contain any scenario information. This will preclude an exercise message being accidentally accepted as a valid threat.

(4) (U) Exercises messages will be Unclassified, preventing compromise of classified information should non-secure circuits be used to pass the exercise message.

b. (U) Commands receiving BLUE DART warnings will immediately acknowledge receipt of the BLUE DART message to the originator and authenticate by executing a call back. The ultimate recipient of the warning will report within two hours through its internal organizational process or SOP, to the USNORTHCOM offices identified below. This report will include DTG of BLUE DART message receipt, from whom received and method of receipt. This report should be made via any of the following circuits to all the offices listed below.

(1) (U) NCOC (24/7 manning):

Classified email: nc.cog.dl@northcom.smil.mil or
nc.cog.chief.omb@northcom.smil.mil

Unclassified email: nc.cog.dl@northcom.mil or
nc.cog.chief.omb@northcom.mil

Message Address: HQ USNORTHCOM PETERSON AFB CO//COG//

Telephone: Commercial (719) 554–2361 (DSN 692–2361)

(2) (U) USNORTHCOM J34:

Classified email: nc.cog.atfp.omb@northcom.smil.mil or nc.j34.omb@northcom.smil.mil

Unclassified email: nc.cog.atfp.omb@northcom.mil or nc.j34.omb@northcom.mil

Message Address: HQ USNORTHCOM PETERSON AFB CO//J34//

Telephone: Commercial (719) 554–8305 / 8311 (DSN 692–8305 / 8311)

c. (U) If a BLUE DART for exercise interferes with a real-world BLUE DART or other time-critical threat warning, any unit involved is authorized to terminate the for exercise BLUE DART. To terminate an exercise, report the following by all appropriate means: “terminate exercise BLUE DART”, and repeat the call. All units involved in the exercise will acknowledge exercise termination back to USNORTHCOM as described in paragraph (b) above. The unit terminating the exercise will also provide the reason for exercise termination.

d. (U) There should never be confusion between actual and exercise BLUE DART messages. An exercise BLUE DART message will never have all three specific criteria areas identified.

e. (U) Exercise Message Formats. This format will be utilized to initiate a BLUE DART exercise from NCOC and is the format to be used by all exercise participants to disseminate messages. (*Annex R, Reports*)

6. (U) BLUE DART Execution Tasks.

a. (U) USNORTHCOM J3.

(1) (U) Establish command-wide AT policy for threat-warning dissemination.

(2) (U) Coordinate with N-NC/J2 to ensure BLUE DART program is properly maintained and exercised.

(3) (U) Monitor DoD Element shortfalls to execute BLUE DART procedures to ensure issues are addressed and mitigated.

(4) (U) Ensure NCOC personnel are properly trained in BLUE DART program procedures.

(5) (U) Issue BLUE DART messages and voice notifications expeditiously upon receipt of applicable intelligence and recognition of reporting criteria.

(6) (U) Develop and maintain checklist(s) for BLUE DART notifications.

(7) (U) Maintain complete and accurate point of contact lists for all DoD Elements organizational 24/7 information points of entry.

(8) (U) Conduct review and analysis on the effectiveness of the program based on feedback from the DoD Elements and After-Action Reviews (AAR) of BLUE DART exercises.

(9) (U) Conduct quarterly BLUE DART exercises.

(10) (U) Maintain, and update as necessary, written policy and procedures for the BLUE DART program.

(11) (U) Ensure procedures are established/maintained to facilitate threat related warning notification from the OIW to the NCOC.

b. (U) Services, USNORTHCOM Subordinate Commands and forces, Defense Agencies and DoD Field Activities TACON (for FP) to USNORTHCOM.

(1) (U) Issue BLUE DART voice notifications and messages to subordinates expeditiously upon receipt.

(2) (U) Ensure threatened units respond expeditiously to receipt of notifications.

(3) (U) Develop local procedures to facilitate rapid dissemination of BLUE DART messages.

(4) (U) Provide and update as required, 24-hour a day/7-days a week point of entry contact information for operations or watch centers identified to receive BLUE DART message traffic.

(5) (U) Ensure NCOC is notified of BLUE DART threat warnings originating from/within the organization.

APPENDIX 2 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
AT POLICY, STANDARDS AND TRAINING REQUIREMENTS (U)

(U) References: *Base Order*.

1. (U) Situation. *Base Order*.

2. (U) Mission. *Base Order*.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) This Appendix will provide definitive guidance regarding AT policy, standards, and training requirements for commands and units deploying forces within the USNORTHCOM AOR. This critical task is a composite of DoDI 2000.16 standards 1, 2, 6, 12, 14, 16-27 and 30 as well as DoDD 2000.12 requirements 5.14.1 to 4, 5.14.6, 5.15.1, 5.15.3, 5.15.4, 5.15.5, 5.15.9, 5.15.10, and 5.17.1 through 5.17.18. The critical requirement for USNORTHCOM and the DoD Elements in the USNORTHCOM AOR is to establish the appropriate processes for coordination to ensure standardization where appropriate, and unity of effort resulting in a coherent, seamless defensive posture in the USNORTHCOM AOR.

(2) (U) Services, Defense Agencies and DoD Field Activities, and USNORTHCOM Subordinate Commands and forces will develop and implement a comprehensive AT Program under their respective control to comply with all the standards contained in DoDI 2000.16, and the requirements of DoDD 2000.12 and DoDI 2000.18, utilizing DoD O-2000.12H as implementing guidance. The standards contained in DoDI 2000.16 are baseline standards and unique requirements may be promulgated in implementing directives to supplement these baseline standards.

b. (U) Tasks.

(1) (U) Commanders at all levels are responsible for the implementation of DoD AT policies within their organizations. USNORTHCOM, Services, Defense Agencies and DoD Field Activities must develop implementing policies to ensure subordinate commanders comply with established requirements or to address policy gaps and seams for the USNORTHCOM AOR.

(2) (U) Coordinate issues concerning policies, standards and training requirements through the NC-FPAO. Proposed changes to policies, standards and training requirements will be formally staffed and coordinated with all DoD Elements operating in the AOR prior to implementation.

(3) (U) Implement Travel and Housing Policies.

(a) (U) Travel Policy**.** USNORTHCOM Travel Policy is established in Appendix 4 to Annex C. The AT Threat level for the USNORTHCOM AOR is determined by N-NC/J2, and dictates the FPCON measures travelers must employ.

(b) (U) Off-Installation Housing.

1. (U) OCONUS.

a. (U) Commanders will ensure all DoD personnel assigned to Moderate, Significant, or High Terrorism Threat Level areas and living in off-installation quarters receive, as a minimum, the guidance in Chapter 22 of *ref. f* for selecting private residences in order to mitigate the risk of terrorist attack. If available, the installation Housing Office should act as the installation or activity Commander's Executive Agent to ensure this AT guidance is provided.

b. (U) Although commanders do not have any specific responsibilities for off-installation housing in areas where the Terrorism Threat Level is determined to be Low, AT planning must include coverage of private residential housing in Moderate, Significant, or High Threat Level areas. Commanders must consider private residential housing in all AT planning to react to changes to the Terrorism Threat Level.

2. (U) CONUS. Applies to off-base housing leased/owned by DoD within CONUS to include AK and PR.

(4) (U) Implement AT Standards. The DoD standards outlined in the DoDD 2000.12 and DoDI 2000.16 apply to all DoD Elements in the USNORTHCOM AOR except those elements and personnel for whom a COM has security responsibility. These standards will be applied by each Service, Defense Agency and DoD Field Activity, and all deployed and mobilized elements operating in the USNORTHCOM AOR where Commander, USNORTHCOM is the supported commander.

(a) (U) The inability to meet minimum DoD and USNORTHCOM AT standards and requirements may result in a higher AT Program risk. Commanders constantly must weigh the risks involved in not complying with the requirements and standards contained in this OPORD. All commanders accepting a higher risk by deviating from this OPORD must seek approval through the chain of command exercising TACON (for FP). Commanders who report directly to HQ USNORTHCOM will seek approval for deviation requests directly from HQ USNORTHCOM.

(b) (U) The DoD Elements will, IAW ref. m, paragraph 1-1.2.3, continue to utilize Service and Agency-specific AT construction and deviation request processes. DoD Elements will submit AT construction deviation requests through their respective Service chains of command to OSD and will provide copies of Service approved deviation requests to USNORTHCOM for the following structures: billeting, primary gathering buildings, and Critical Facilities (ref UFC 4-010-01, paragraph 1-5.3).

Commander, USNORTHCOM retains the right to review and make change recommendations to OSD on these deviation requests.

(c) (U) All Service, Defense Agency, DoD Field Activity and other Combatant Command personnel in the USNORTHCOM AOR for whom Commander, USNORTHCOM has AT responsibility ensure command standards address the following areas:

1. (U) Procedures to collect and analyze terrorist threat information, threat capabilities, and vulnerabilities to terrorist attacks.

2. (U) Terrorism Threat Assessments, Risk Assessments, and AT Plans to Include Terrorist Incident Response and Terrorist Incident Management measures.

3. (U) Procedures to enhance AT protection, which might include but are not limited to, training programs, awareness campaigns, and technology applications.

4. (U) Procedures to identify AT requirements and to program for resources required to meet security requirements.

5. (U) VAs and a process to address, track, and mitigate vulnerabilities.

(5) (U) Assignment of Antiterrorism Officers (ATO).

(a) (U) Installation/Site Commanders will designate in writing a commissioned officer, noncommissioned officer or civilian staff officer as the ATO for each installation, base and deployed site battalion, squadron or larger (to include Navy ships) under their command. The designated ATO will be trained in AT procedures in a formal Service-approved Level II AT course. Subordinate HQs Commanders must develop a process to verify units deploying into or transiting through the AOR have a trained, assigned ATO.

1. (U) Antiterrorism Officer (ATO) will:

a. (U) Meet the following criteria:

1) (U) Be an officer, noncommissioned officer, or DoD civilian assigned in writing to be the major command or unit/installation ATO.

2) (U) Be Level II trained through a Service, or other, resident or Mobile Training Team (MTT) Level II course.

b. (U) Be responsible for managing a comprehensive AT Program and advising the commander on all AT issues.

c. (U) Provide and track Level I Awareness Training for unit personnel.

d. (U) Understand requirements for developing, exercising, and assessing AT plans in accordance with DoDI 2000.16 standards and this OPORD.

e. (U) Prepare AT plans for the unit/site utilizing the Joint Antiterrorism Program Manger's Guide resident within ATEP meets all requirements for developing an AT plan when used in its entirety.

f. (U) Installation ATO will coordinate through the installation ATWG or equivalent to ensure AT considerations are addressed in contractor background checks, facility/site selection and construction criteria.

(6) (U) FPCON Measures Implementation. Commanders will ensure that FPCON transition procedures and measures are properly disseminated and implemented in facilities under the control of DoD. In facilities outside DoD authority and jurisdiction, (GSA facilities, etc.) facilities will implement the DHS Threat Advisory protocols.

(7) (U) DoD Elements Will Maintain a Comprehensive AT Program.

(a) (U) The AT Plan and supporting elements will clearly describe site-specific AT measures. These directives will be based on the guidance contained in DoD, Service, and Combatant Command publications and this OPORD and should be written from the DoD Element level to the installation level for permanent operations or locations, and incorporated in Operations Orders for temporary operations or exercises.

(b) (U) At a minimum, AT Plans and/or OPORDs will address the key elements discussed in Chapter 9 of *ref. aa*.

(8) (U) DoD Elements Will Establish AT Physical Security Measures.

(a) (U) AT Physical Security measures will be addressed, supported, and referenced within the AT planning directive to ensure an integrated approach. Commanders must develop a physical security plan for personnel and facilities under their authority to include procedures to:

1. (U) Detect possible hostile intent, activities, or circumstances.

2. (U) Assess the potential threat.

3. (U) Delay any unauthorized activity, persons to circumvent physical security measures.

4. (U) Deny access, capability, or opportunity to create circumstances that could lead to loss of life or damage to mission-critical resources.

5. (U) Notify appropriate personnel to take action.

(b) (U) AT plans will integrate facilities, equipment, trained personnel, and procedures into physical security measures as part of a comprehensive effort designed to provide maximum AT to personnel and assets. This may be accomplished through the development of a synchronized AT matrix that outlines who will do what, where, when, and how.

(c) (U) All physical security measures must include procedures for the use of physical structures, physical security equipment, and security procedures, Random Antiterrorism Measures (RAM), response forces, and emergency measures sufficient to achieve the desired level of AT protection and preparedness to respond to a terrorist attack.

(9) (U) DoD Elements Will Establish Terrorist Incident Response Measures.

(a) (U) Installation Commanders, afloat Commanders and responsible DoD officials will prepare installation, shipboard, or DoD-occupied facility terrorist Incident Response Measures. These measures will include procedures for determining the nature and scope of post-incidence response and steps to reconstitute the ability to perform the unit's mission while providing an appropriate level of AT.

1. (U) Terrorist Incident Response measures should address the full scope of response to a terrorist incident. The nature of the response will depend on many factors. The character of current operations at the time of the terrorist incident will have significant bearing on the scope, magnitude, and intensity of response.

2. (U) Terrorist Incident Response measures are ineffective if not fully coordinated, exercised, and evaluated. Commanders must ensure all emergency response forces (security, fire, medical) and recovery forces (engineers, logistics, etc.) fully integrate their responses into a coordinated plan. Commanders should conduct frequent drills to familiarize all personnel with individual responsibilities during an emergency.

3. (U) Commanders in Moderate, Significant, and High Terrorism Threat Level areas will ensure terrorism Incident Response measures contain current residential location information for all assigned DoD personnel and their family members. Such measures should provide for enhanced security and/or possible evacuation of DoD personnel and their family members. Furthermore, Commanders in such areas should investigate special security arrangements to protect DoD personnel and their family members living on the civilian economy. Close coordination with other U.S. Government agencies is essential to ensure effective allocation of security resources and protection.

(10) (U) DoD Elements Will Establish Terrorist Incident Management (IM) Measures.

(a) (U) Commanders must include terrorist IM preparedness and response measures as an adjunct to the installation AT planning directive.

1. (U) The Terrorist IM measures must include the C3 process for emergency response. The measures also must include disaster planning/preparedness procedures outlining the response of various organizations (installation/base engineering, logistics, medical, mass casualty response, transportation, personnel administration, and local/ host nation support). In addition, the nature of a terrorist attack may require broader responses that include higher levels of authority or command. For example, terrorist use of WMD, or terrorist attacks on dignitaries while visiting DoD installations, will require immediate close coordination with higher commands, civilian authorities, host nation authorities, and the COM.

2. (U) The IM procedures may be included in other plans (Mass Casualty Plan, Disaster Response Plan, Base Defense Plan, etc.) and do not necessarily need to be included in the installation AT Plan. However, the AT Plan must provide guidance or reference to the appropriate plan.

(11) (U) DoD Elements will conduct AT Program Reviews.

(a) (U) Commanders at all levels will review their own AT Program and plans at least annually to ensure compliance with directives and to continuously improve the AT Program. For the same purpose, commanders at all levels will likewise conduct a documented compliance review of the AT Programs and plans of their immediate subordinates in the chain of command at least annually. (*Appendix 6, AT Vulnerability and Program Assessments*)

(12) (U) DoD Elements Will Implement AT Training Requirements.

(a) (U) Installation/Site Commanders (including Navy ships) will conduct annual field and staff training that exercises the AT Plan.

(b) (U) Training.

1. (U) General Requirements for AT Training. Commanders will ensure all assigned personnel receive appropriate training to increase AT awareness. Individual records will be updated to reflect AT training in accordance with Service policy and guidelines.

2. (U) Level I AT Awareness Training will be provided to all DoD personnel (to include DoD contractors) and their family members annually, per DoDI 2000.16, Standard 22. Commanders will ensure that every military Service member,

DoD employee, and local national hired by the Department of Defense, regardless of rank, is made aware of the need to maintain vigilance for possible terrorist actions and employ AT tactics, techniques and procedures, as discussed in DoD O-2000.12-H and Joint Pub 3-07.2. Commanders also will offer Level I AT Awareness Training to contractors employed by the DoD, consistent with the terms and conditions specified in the contract.

3. (U) Commanders will ensure all DoD personnel and their family members deploying/traveling on official government orders to and within the USNORTHCOM AOR receive Level I AT Awareness training and other antiterrorism training as may be required by Appendix 5 to Annex C.

4. (U) Theater and country clearance granting authorities will not approve official travel to the USNORTHCOM AOR unless Level I AT Awareness Training and AOR-specific training has been verified/accomplished before departure from home station. Personnel from other Combatant Commands and those personnel traveling OCONUS within the USNORTHCOM AOR are required to complete Level I training before official travel to the USNORTHCOM AOR.

5. (U) Training for High-Risk Personnel (HRP) and High-Risk Billets. HRP are eligible for advanced AT training. In some instances, this training may be extended to include family members.

6. (U) Services retain responsibility for Level III AT training allocations. All DoD Elements retain responsibility for Level IV AT training allocations.

a. (U) Chapter 18 of *ref. aa* contains information regarding Level III (Pre-command AT Training) and Level IV (Executive Seminar).

b. (U) The Joint Staff designates Combatant Command and Service quotas and is responsible for conducting Level IV training. USNORTHCOM will manage allocated slots for the USNORTHCOM Headquarters and COCOM/OPCON elements. DoD Elements will continue to manage their own allocations. DoD Elements within the USNORTHCOM AOR will provide NC/J34 with a list of attendees.

(13) (U) Designation of High-Risk Billets (HRB) and High-Risk Personnel (HRP).

(a) (U) Commanders will recommend the designation of HRB and personnel at high risk to terrorist attack (HRP). Such recommendations will be based upon Service guidelines and a continuing review of the terrorist threat and other circumstances related to the individual or position. Approval authority for such designations normally will not be delegated below the Supporting Service Commander level. In the case of DoD personnel/positions not assigned to a Supporting Service Command, Deputy Commander, USNORTHCOM will retain this authority. Other Combatant Commanders will retain the authority to designate high-risk billets and

individuals relative to assigned forces. However, for personnel visiting the USNORTHCOM AOR, a general or flag officer in the chain of command of the hosting unit may make such determinations, or in the absence of a hosting unit, the USDR for the country being visited.

(b) (U) Commanders will forward a listing of HRP and billets to NC/J34 as directed annually and provide updates as changes occur.

APPENDIX 3 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
AT EXERCISE PROGRAM (U)

(U) References: *Base Order*.

1. (U) Situation. *Base Order*.

2. (U) Mission. *Base Order*.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) The requirements for AT training and exercises are articulated in DoDI 2000.16, standard number 19. This critical task specifically addresses the DoDI 2000.16 standard, DoDD 2000.12 requirements 5.14.1, 5.15.1, 5.17.1, 5.17.2, 5.17.4, 5.17.5, 5.17.8, 5.17.9, 5.17.10, 5.17.11, 5.17.12, 5.17.16, 5.17.17, and 5.17.18 as well as specific USNORTHCOM requirements.

(2) (U) The DoD Elements in the USNORTHCOM AOR will conduct a minimum of one AT exercise incorporating some aspect of CBRNE preparedness annually. This combined AT/CBRNE exercise can be conducted separately or in conjunction with the annual AT exercise requirement. More frequent exercises may be required depending on the local terrorist threat. The scope, type, methodology, length, and execution of this exercise are at the discretion of the assigned Commander, Service, Defense Agency or DoD Field Activity. The exercise should incorporate the most recent and/or likely terrorist threat scenarios currently in existence. It is understood that facilities located off DoD installations have limited ability and capabilities to conduct CBRNE exercises, but CBRNE preparedness will be exercised annually, at a minimum.

(3) (U) AT plans are not considered to be validated or executable until they have been exercised through the IM and recovery phase. Compliance with the AT and AT/CBRNE exercise requirement will be assessed by the DoD Element and communicated via an annual AT exercise report, in terms of a percentage of installations/facilities in compliance with the exercise requirement, and a by-name list of installations/facilities not in compliance with the reason, to Commander, USNORTHCOM, due 1 October. (*Annex R, Reports*)

(4) (U) NC/J34 will coordinate with assigned forces, Services, Combatant Commands, Defense Agencies and DoD Field Activities to include them as an integral part of USNORTHCOM training and exercise scenarios and planning IAW Commander's Training Guidance. NC/J34 will maintain appropriate liaison with N-NC/J7. NC/J34 will coordinate with the assigned forces, to include them as an integral part of USNORTHCOM Level 1 (USNORTHCOM Staff training) and Level 2 (Joint Task Force training) exercise scenarios and planning IAW USNORTHCOM Commander's Training Guidance.

(5) (U) AT plan exercises will be provided the same emphasis afforded combat task training and executed with the intent to identify shortfalls impacting the protection of personnel and assets.

b. (U) Tasks.

(1) (U) Pre-Deployment AT Exercise. Commanders will ensure, as part of pre-deployment requirements, that an AT exercise is conducted to validate the pre-deployment AT plan. Report completion of exercise to next higher headquarters.

(2) (U) Incorporating AT Planning Into Exercises.

(a) (U) AT must be included as an integral part of exercise scenarios and planning. When conducting AT mission analysis and planning, the ATO must include AT as part of the tactical mission. Portions of the AT plan can be exercised more frequently and during each increase in FPCON during duty and non-duty hours. This will ensure that the physical security portion of the AT Program is consistent with local FPCONs. Exercises should involve security, fire, medical, explosive ordnance disposal, disaster preparedness/emergency management, and local agencies to the greatest extent possible.

(b) (U) DoD Elements with overall responsibility for coordination, planning, and execution of an exercise conducted in USNORTHCOM AOR will:

1. (U) Ensure an AT plan is developed for the exercise.

2. (U) Identify and include AT requirements into the Joint Operation Planning and Execution System (JOPES) Time-Phased Force Deployment Data (TPFDD) planning to ensure transportation feasibility.

3. (U) Identify AT concerns early in the planning process and develop mitigating measures. Consider sending FP assessment teams into an area before deployment if the situation warrants this action.

4. (U) The ATO will:

a. (U) Serve as the Commander's focal point for planning, coordination, and execution of real world AT planning.

b. (U) Develop the AT plan. See Tab A for a Sample Exercise AT Plan Format.

5. (U) Supporting Agencies (including other Headquarters and units participating in an exercise) will:

a. (U) Be responsible to the Commander for executing their portion of the Exercise AT Plan.

b. (U) Adhere to all requirements of the exercise AT Plan.

(c) (U) AT scenarios/injects will be incorporated into larger exercises in order to extract the maximum training benefit for all concerned. Given the frequency of joint operations in the USNORTHCOM AOR, AT procedures should be practiced during such operations in order to resolve interoperability issues.

Tab:

A. AT Exercise Plan Format (U)

APPENDIX 4 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
IN-TRANSIT SECURITY AND FORCE TRACKING (U)

(U) References: *Base Order*.

1. (U) Situation. *Base Order*.

2. (U) Mission. *Base Order*.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) To provide policy and guidance regarding AT requirements for DoD Elements, personnel and assets conducting intra-theater/inter-theater transit, referred to as in-transit forces, within the USNORTHCOM AOR. In-transit forces for the purpose of this Appendix include all DoD ships and aircraft, and DoD Elements that could present lucrative terrorist targets; minimally those elements, units or groups consisting of more than 50 personnel. Commanders may lower this threshold of unit size at their discretion. USNORTHCOM will establish the process to effectively coordinate, standardize and synchronize the associated AT requirements. This task is derived from DoDI 2000.16 standards 1-6, 11-15, 22-23, 27, and 31; also DoDD 2000.12 requirements 5.17.1 through 5.17.13 and 5.17.16 through 5.17.18.

(2) (U) The Commander of a U.S. element always remains responsible for the protection of his unit regardless of location. In the current threat environment, intra-theater transiting forces require the same degree of attention as other transiting units to deter, disrupt and mitigate acts of terrorism. Commanders with FP responsibility for a transiting force, within the USNORTHCOM CONUS when in support of USNORTHCOM, or OCONUS in the USNORTHCOM AOR only (and as required by Commander, USNORTHCOM based on the threat), shall ensure the development and execution of in-transit security plans when, based on the current threat environment and assessment, the commander feels his unit is a lucrative terrorist target. This planning process, in addition to the use of Service specific operational risk management planning techniques, will measure the activity against the risk to the in-transit element and will enable the Commander whether to suspend or continue the transit.

(3) (U) Commanders with FP responsibility for a transiting force will ensure the execution of pre-deployment AT vulnerability assessments (VA). This includes movement routes that may be used by transiting DoD forces, ships, aircraft, and DoD personnel on official travel.

(4) (U) Since a variety of factors could affect the timing of assessments for in-transit forces, no specific timeline is established. The intent is to conduct assessments sufficiently in advance of missions to facilitate development of security procedures,

acquisition of necessary materials, tailored and focused intelligence, security support augmentation (if necessary), and coordination with the host nation/interagency, but within a timeframe that provides the commander with current situational information. Thus, an original assessment significantly in advance of a deployment may necessitate a follow-on validation prior to the deployment.

(5) (U) Assessments of ports and airfields will be accomplished for DoD ships and aircraft regardless of the threat level. Assessments are conducted by the Services, the Naval Criminal Investigation Service (NCIS), or the USAF Office of Special Investigations (AFOSI) FP teams. On-scene pre-deployment assessments of locations where the Terrorism Threat level is Low or Moderate will be at the discretion of the responsible commander unless otherwise specified.

(6) (U) Deploying commanders will implement appropriate AT measures to reduce risk and vulnerability. If warranted, commanders faced with emergent or emergency AT requirements prior to movement of forces should submit CbT RIF requests through established channels to procure necessary materials or equipment for required protective measures.

(7) (U) Appendix 6 of *ref. f* contains an AT Planning Requirements Matrix designed to help the Commander determine AT planning requirements when developing in-transit forces security plans.

b. (U) Tasks.

(1) (U) DoD Elements will:

(a) (U) Ensure deploying Unit Commanders comply with the pre-deployment requirements outlined in Tab A.

(b) (U) Ensure an AT plan is prepared for each deployment. A deploying element is a battalion/squadron or larger deploying OCONUS, or in CONUS in support of USNORTHCOM. See Tab B.

(c) (U) Establish policies as required to ensure compliance with DoD and USNORTHCOM requirements for in-transit security of units and personnel.

(d) (U) Establish Threat Working Groups (TWG) or comparable forum. The role of a TWG is to review intelligence and vulnerability assessment (VA) information for in-transit locations, conduct a risk assessment, develop security policies and procedures, develop risk mitigation measures, and make "Go/No Go" mission recommendations to approving authorities.

(e) (U) Ensure all assigned and/or attached personnel review and comply with the USNORTHCOM Travel Policy (Tab A) and Travel Policy Briefing at https://www.noradnorthcom.smil.mil/j3/j34/ or

https://www.noradnorthcom.mil/j3/j34/,.and submit a Travel Clearance Request IAW *ref. k*.

(f) (U) Develop location specific FPCON measures or actions for each FPCON. Utilize organic intelligence resources, situational awareness and understanding of unit capabilities to detect specific and tailored measures to be implemented at specific sites for both stationary and in-transit units. This information will be maintained at the classification level of Confidential or above.

(g) (U) Ensure deploying units coordinate with the USDAO to the host nation IAW the DoD Foreign Clearance Guide, *ref. k*. See Tab B.

(h) (U) Ensure RAMs/security measures are developed for each FPCON and periodically implemented for in-transit units.

(i) (U) Provide direct AT support to in-transit units:

1. (U) Track all in-transit units as they transit through the USNORTHCOM AOR.

2. (U) Provide tailored terrorist threat intelligence. Prior to the deployment, provide detailed threat briefings to enhance situational awareness and AT preparedness.

3. (U) Employ countersurveillance and CI resources in support of in-transit units.

4. (U) Provide threat assessments and VA of routes and sites used by in-transit forces.

5. (U) Direct tailored FPCON measures to be implemented by in-transit units at specific locations.

6. (U) Assist in-transit units in tailoring AT plans based on regional SA.

7. (U) Provide AT augmentation as required. Provide onboard and/or advance-site support prior to and during visits to higher-threat areas of Significant or High Threat Levels, or where a geographically specific Terrorism Warning Report is in effect. This includes ports, airfields, and inland movement routes that may be used by in-transit forces. Providing this augmentation is necessary in order to provide security, site surveys and assessments, CI and countersurveillance support, and to act as liaison with the country team, host nation's security force, contractor and port authority. Such advance-site support will also allow the opportunity to communicate current local threat information to in-transit units, enabling the onboard AT team to more effectively tailor AT measures to the specific threat environment.

8. (U) Develop and implement an Operational Risk Management (ORM) assessment for each installation and each in-transit and intra-theater unit movement.

(2) (U) Parent Organizations of In-Transit Forces will:

(a) (U) Track the movement of all in-transit subordinate elements and personnel on official orders within the USNORTHCOM AOR (through JOPES).

(b) (U) In coordination with supporting intelligence organizations, ensure that focused and tailored terrorist threat information is disseminated to in-transit forces.

(c) (U) Require assigned in-transit forces to engage in the risk assessment management process before deploying to, or within, the USNORTHCOM AOR.

c. (U) Coordinating Instructions.

(1) (U) In-Transit Aircraft Security Procedures.

(a) (U) An Airfield Assessment Checklist is provided in Tab B to Appendix 6. The guidance in this OPORD represents a minimum level of physical security for aircraft, but personnel should refer to airframe security standards to determine specific requirements.

(b) (U) This section applies to all DoD or DoD-chartered elements, aircraft and accompanying personnel operating in the USNORTHCOM AOR under the AT responsibility of Commander, USNORTHCOM.

(c) (U) The DoD Elements with AT responsibility will ensure:

1. (U) Continuous contact with aircraft transiting the USNORTHCOM AOR is maintained.

2. (U) Airfield security/VAs are accomplished every three (3) years and ensure results are entered in the CVAMP database. *See Appendix 6, AT Vulnerability and Program Assessments*.

3. (U) All OCONUS airfield assessments are coordinated through the appropriate USDR. Tab C, USDR/USDAO Country Points of Contact.

4. (U) Aircraft deploying to an OCONUS location contact the USDR or Embassy RSO to ensure proper security requirement arrangements are made in advance of arrival. Normally will be accomplished via message traffic, and may be included in the theater/country clearance request message.

5. (U) The responsible USDR and/or U.S. Embassy RSO will ensure the security requirements outlined in paragraphs 6 through 13 are implemented when requested via message traffic or theater/country clearance request message.

6. (U) Some form of unimpeded escort for the aircraft to and from designated parking location.

7. (U) Aircraft parking locations will be a minimum of 100 meters (300 ft) from the airfield perimeter, other buildings or aircraft on the ramp.

8. (U) Organic/contracted security forces immediately establish a security zone, encompassing the entire aircraft maintaining a minimum distance of 35 meters (100 ft) using elevated ropes/stanchions (if available) or similar equipment, unless available from the aircrew.

9. (U) Organic/contracted security forces prevent personnel or equipment from entering the security zone until cleared by a U.S. crewmember.

10. (U) Appropriate security is available for crew to conduct duties as required. This may entail escorting while on the airfield as well as transiting to and from off-airfield areas; e.g., meeting locations, hotels, etc.

11. (U) If the aircraft must remain overnight (RON), ensure the following additional measures are provided:

a. (U) Based on the FPCON level and current Threat consider a 24-hour manned access control point and continuous patrol coverage (e.g., random armed patrol coverage in addition to the armed security/escort personnel, not to exceed every 2 hours, and an armed response to incidents affecting aircraft security within 5 minutes of notification of the need for such response).

b. (U) Arrange for lodging of crew at a DoD- or DoS-approved/recommended facility.

12. (U) Airfield Categories (CAT) in CONUS. In CONUS airfields are divided into two categories:

a. (U) CAT 1 airfields do not normally require additional security.

b. (U) CAT 2 airfields normally require additional security.

CAT 1	CAT 2
US military controlled	International/Regional Airport with inadequate or questionable security

International/Regional Airport with adequate security confirmed	Bare base

Figure C-4-1

13. (U) Airfield Categories (CAT) OCONUS. OCONUS airfields are also divided into two categories:

a. (U) CAT 1 airfields do not normally require additional security.

b. (U) CAT 2 airfields normally require additional security.

CAT 1	**CAT 2**
US military controlled	Host Nation military controlled with inadequate or questionable security
Host Nation military controlled with adequate security confirmed	International/Regional Airport with inadequate or questionable security
International/Regional Airport with adequate security confirmed	Bare base

Figure C-4-2

c. (U) Transient Operations to Security CAT 1 Airfields**.** CAT 1 airfields do not normally require security augmentation for routine operations under normal circumstances. Exceptions to this may occur in the event intelligence indicates a specific terrorist threat to the location. Additional security should also be planned for high visibility transits and large-scale unit deployments. Special circumstances, mission criticality, heightened Terrorism Threat Level, Defense Terrorism Warning Report issuance, or increased FPCON level, may cause an airfield to move from CAT 1 to CAT 2 designation.

d. (U) Transient Operations to Security CAT 2 Airfields. The following provides general policy for agencies and crewmembers when planning and executing aircraft security/force protection measures at CAT 2 airfields. In some situations, the limitations levied by host nations may affect the ability to achieve these measures. Aircrews, mission commanders, and security personnel must strive to meet these baselines wherever possible.

(d) (U) Prior To Departure.

1. (U) The aircrew and security personnel will receive a tailored, comprehensive planning package that, beyond standard flight planning information, includes a summary of threats along the route of flight, at the terminal area and the airfield. The package will also contain U.S. Embassy Country Team information to include RSO contact numbers/names, USDR (who usually is the DATT), contact numbers, and how to contact local/contracted security at the airfield of intended destination, if applicable. Imagery/maps of the airfield, if available, should indicate the

likely parking location so that the aircrew and security personnel can determine escape routes should they become necessary. The package should include by name, the person who will meet the aircraft in order to provide liaison and security updates at the time of arrival. If operating at a civilian airfield, the package should include the name of the companies that will be providing aircraft servicing. If security arrangements are deemed inadequate, or not in compliance with this operating order, the aircraft commander should attempt to resolve the issue with local officials. If not resolved, the aircraft commander must bring the situation to the attention of their C2 agency.

2. (U) If the airfield requires onboard security personnel to accompany the mission (Armed Escorts/Security Forces), the security team leader (STL) will be present and participate in the aircraft commander's mission briefing. Security personnel will cover standard briefing items to include how they will operate when the aircraft arrives, and to confirm signals and other means of communicating with the crew prior to the crew leaving their seats after engine shutdown. They will brief on the carrying of weapons (armed/covert/overt) during the mission to include the Rules for the Use of Force (RUF). The designated Supporting Service Commander element, TWG, STL or aircraft commander will make contact with a member of the U.S. Embassy Country Team NLT 24 hours prior to departure for current airfield information. Supporting Service Commanders will determine the appropriate coordination procedures with Country Teams to ensure adequate exchange of information without unnecessary and redundant interactions.

3. (U) If required, security for the aircraft will be conducted on a 24-hour basis. Aircrews and mission planners should plan accordingly.

4. (U) When the type or size of the aircraft does not permit on-board security personnel the supporting commander will request additional host airfield security support or send advance U.S. security elements. When existing airfield support will still not satisfy DoD/USNORTHCOM requirements and DoD-provided security is not feasible, the respective TWG will advise the appropriate commander for a decision regarding execution of the mission.

(e) (U) Enroute. From an FP standpoint, there must be continuous en route voice communication capability between DoD aircraft and their corresponding C2 organization. The C2 organization must be able to maintain continuous contact with transiting aircraft. The C2 organization must be able to pass updated threat information to its aircraft en route, possibly leading to an en route change of destination.

(f) (U) Airfield Arrival, Security and Departure Procedures. Services will ensure aircraft security standards are provided to supplement this operating procedure and properly secure aircraft on the ground.

(g) (U) Off-Airfield Activities. If crewmembers or passengers are to use rental vehicles, they should only be procured from reputable agencies, or a U.S. Country Team recommended/contracted dealer when such information is available. Prior to

loading, starting, or driving a rental vehicle, personnel should conduct a thorough inspection of each vehicle using DoD checklists to ensure each vehicle has not been tampered with. Crewmembers should only stay in lodging facilities recommended by DoS or local U.S. military officials, when such information is available. Crewmembers should conduct inspections of their rooms using DoD-approved checklists. Rooms should also be reexamined when returning and vehicles reexamined after being left unattended. Throughout the time on the ground, aircrew members and their passengers must ensure complete control over their personal belongings to ensure that no foreign-objects/devices are introduced.

(2) (U) In-Transit Ship Security.

(a) (U) This section applies to all DoD or DoD-chartered elements, ships and accompanying personnel operating in the USNORTHCOM AOR under the AT responsibility of Commander, USNORTHCOM.

(b) (U) The DoD Elements with AT responsibility will ensure:

1. (U) U.S. Naval vessels, Naval Fleet Auxiliary Vessels, Military Sealift Command Vessels, and Combat Logistics Forces Tactical Control (TACON) to Commander, USNORTHCOM for AT protection. An example of this category would be a submarine from SUBLANT during a port visit within the USNORTHCOM AOR.

2. (U) Commander, USNORTHCOM and subordinate commanders exercise no AT authority or responsibility for commercial vessels chartered by DoD, unless specifically provided for in the contract. When such vessels carry vital DoD material or DoD personnel (supercargo), Commanders will request threat assessments from supporting intelligence organizations and conduct a threat analysis/risk assessment to determine port security requirements.

(c) (U) Port Visit Requirements.

1. (U) Services commands must be able to maintain continuous contact with transiting ships. Services will identify shortfalls in en route communications capabilities and will take steps to maintain contact with ships anywhere in the USNORTHCOM AOR. Inability to satisfy this requirement will be reflected in executive/operations orders and considered during mission planning and approval, but does not require submission of a waiver request to HQ USNORTHCOM.

2. (U) Supporting Service Commanders and Task Force commanders will ensure CONUS port installations have had a VA within the past three years before allowing their forces to use them. If a VA has not been conducted, a VA will be conducted before being used and CVAMP will be updated and USNORTHCOM NC/J34 will be advised of the update.

(d) (U) Transient Operations.

1. (U) AT planning must be conducted for each port visit including brief stops requiring mooring, anchoring or operating in confined locations. AT planning also is required for transiting restricted straits, canals and waterways. As a minimum, Port Visit AT planning includes items 2-5, below.

2. (U) Assessments**.** Threat and Port VA are key elements in the planning process and provide commanders a foundation for preparing their In-port Security Plans (ISP).

3. (U) In-Port Security Plans (ISP). Ships will develop ISPs, which should include all measures applicable to the current FPCON level. They should focus on employing non-lethal means first (barriers, fire hoses, etc.), use whatever reasonable necessary and proportional force (up to and including deadly force) to counter the threat. Measures implemented onboard the ship may be employed at the Commanding Officer's discretion. Specific AT measures that fall into this category are those from a higher FPCON level that occur off ship and/or require host port support.

4. (U) AT Logistics Request (LOGREQ) Supplement. While in FPCON BRAVO or higher, ships are to request support via separate LOGREQ. This procedure enhances AT.

5. (U) Water Borne Security. Each ISP should include measures to establish clear lines of demarcation (e.g., posted warnings, booms, or buoys) to create standoff and to define protective concentric zones of defense around the ship. In situations where the host port does not permit visible demarcation lines, ships are to implement other means to identify the defensive zones to security response personnel. The innermost area will be a standoff distance within which only identified and authorized personnel are permitted. Outside this area will be three additional concentric perimeters. From the outside–in, these perimeters will be the outer borders of:

a. (U) Assessment zone. Detect, localize, track, classify, inspect, identify and "tag" intruders as authorized, unauthorized, or unknown.

b. (U) Warning zone. Hail, warn away, or intercept unauthorized and unknown intruders.

c. (U) Threat zone. Using all known facts, determine if contact has demonstrated hostile intent or committed a hostile act. If hostile intent or hostile actions are perceived, use whatever reasonable force may be necessary (up to and including deadly force) to decisively counter the threat. If, in the opinion of the decision-maker, the perceived threat would not be significantly increased, engage with non-lethal weapons (charged fire hoses, etc).

(3) (U) In-Transit Ground Forces Security. In-transit ground force security for forces transiting OCONUS and all transiting forces in support of USNORTHCOM; or,

when directed by Commander, USNORTHCOM for higher threat levels in CONUS; Level I training remains a requirement.

(a) (U) Commanders will establish policies and procedures for a formal process to assess risk when traveling OCONUS in the USNORTHCOM AOR, including specific approval authority for each level of risk.

(b) (U) Before movement, commanders must conduct a terrorist threat assessment and vulnerability assessment of all locations and routes their troops will transit, including arrival sites, movement routes, planned halts, and departure sites.

(c) (U) After conducting a preliminary assessment, which normally includes checking available ground, airfield and port databases, commanders must determine if an on-site FP assessment is required. Assessment team composition is mission and location dependent, with specific functional area representation including operations, intelligence, CI, physical security, engineer, chemical, medical and other specialties as required. Commanders should request support from higher headquarters for transit operations through ports or airfields requiring expertise beyond the ability of the commander to provide internally.

(d) (U) Tab A to Appendix 6 to Annex C, is a guide for use in conducting pre-deployment assessments and developing mission security measures. Although not all items will apply to every type of movement, the checklist provides a detailed list of FP-specific considerations related to ground transit operations.

(e) (U) Threat/Risk Management. Based on information provided during the threat and vulnerability assessments, operational commanders identify specific measures designed to reduce risk. These measures form the basis of the movement security plan.

(f) (U) Commanders will develop a movement security plan focused on in-transit operations and synchronize this plan with the overall movement plan. The security plan must include specific measures addressing:

1. (U) Security at arrival sites, on movement routes, during planned halts, and at departure sites. Address route planning, vehicle requirements, weapons and equipment requirements, night vision equipment, and vehicle escort and movement requirements. For repetitive movements, consider varying routes and times to prevent establishing a routine that facilitates terrorist planning. Plans for movement should also include the following:

a. (U) Procedures for maintenance recovery operations, including security of the recovery team.

b. (U) Procedures for medical evacuation, including security of the medical team.

c. (U) Elements must establish a clear chain of command for movement. The commander (or senior officer present) is responsible for ensuring security measures adequately address vulnerabilities. Transiting elements should establish secure communications with an operations center capable of coordinating response operations.

d. (U) RUF for each area that the element will transit or occupy.

(g) (U) Thorough mission planning includes determination of critical information – essential elements of friendly information (EEFI) that must be safeguarded from unauthorized or inadvertent disclosure. Following analysis of OPSEC indicators and vulnerabilities, assess the threat to U.S. forces and decide what level of risk to assume. Finally, incorporate appropriate OPSEC procedures into the overall security plan to ensure the protection of information critical to U.S. forces and the mission. OPSEC applies not only to protecting information during the planning stages of an operation, but during the operation as well.

(h) (U) Ground transit operations in the USNORTHCOM AOR may involve an Aerial Port of Debarkation (APOD) or Sea Port of Debarkation (SPOD).

(i) (U) Routes between arrival points and destination points must be assessed. Consider mission profile and terrorist threat in determining the level of detail for the assessment. Higher threat areas may require a thorough route reconnaissance prior to movement, while a map reconnaissance may suffice for lower threat areas.

(j) (U) The Unit Commander (or senior officer accompanying the movement) is responsible for the implementation of the movement security plan. This includes continuous assessment of the threat during the operation and revision of the plan as necessary to mitigate emerging vulnerabilities during movement.

(k) (U) Transiting elements must complete all required training before arrival in theater or movement. Although parent units are responsible for training their forces, the Commander responsible for FP during the operation must ensure all forces have completed the required training. See Tab A to Appendix 5 of Annex C for all mandatory training and pre-deployment requirements.

(4) (U) Individual and Small Group Travel. Appendix 6 to ref. f contains guidelines and an AT planning process for individual and small group travel (less than 50).

Tabs:
A USNORTHCOM Travel Policy (U)
B AT Plan for Deploying Units (U)
C USDR/USDAO Country Points of Contact (U)

TAB A TO APPENDIX 4 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
USNORTHCOM TRAVEL POLICY (U)

1. (U) USNORTHCOM Pre-deployment Anti-Terrorism/Force Protection (AT/FP) Training Requirements.

a. (U) Categories of travel. USNORTHCOM classifies all travel into three categories: official travel (PCS, TDY/TAD, deployments), unofficial individual travel (personal leave), and unofficial DoD-sponsored group travel. In some cases, it may be difficult to determine precisely which a specific traveler falls into. In such cases, address any questions to the USNORTHCOM Theater Clearance Manager (NC/J34) at DSN 692-8307, commercial (719) 554-8307, or fax 692-7132. Pre-deployment and FP training requirements and the theater clearance approval report are available on the USNORTHCOM home page at http://www.noradnorthcom.smil.mil/j3/j34. The following USNORTHCOM AT/FP training requirements apply to all categories of travel unless otherwise specified. All DoD personnel traveling to any location OCONUS in the USNORTHCOM AOR must complete the training listed below regardless of how long their travel lasts, and their travel request message must include a statement that they have met each of the training requirements specified. All DoD personnel traveling to any location OCONUS that is within the USNORTHCOM AOR must complete the training listed below. They must do so regardless of how long their travel lasts, and their Travel Clearance Request message must include a statement that they have met each of the training requirements specified.

b. (U) Level I AT/FP Training. All personnel traveling to the USNORTHCOM OCONUS AOR must receive required Level I AT/FP training (classroom instruction or required reading) from their parent unit or command prior to deployment or initiating travel. This training must be provided by personnel qualified to AT/FP Training Level II or by web-based training approved by a service or a combatant command. Approved web-based training is available at https://www.at-awareness.org/. The access code is "aware" (no quotes). Users employ a self-generated user ID and password to proceed to the training, which lasts 30-45 minutes. Travelers may also be required to undergo additional training in AT awareness specific to the place(s) to be visited. See DoDI 2000.16 for specific Level I AT/FP training requirements.

(1) (U) Eligible Family Members. Eligible family members 14 years and older (or younger, at the discretion of the DoD sponsor) traveling on official business (i.e., on an accompanied permanent change of station move) to countries in the USNORTHCOM AOR OCONUS must receive Level I training prior to their departure in accordance with DODI 2000.16.

(2) (U) Contractor Employees. DoD Elements offer Level I training to contractor employees under terms and conditions specified in the contract.

(3) (U) USNORTHCOM Personnel. NC/J34 provides Level I training for USNORTHCOM personnel if the directorate of the individual or group does not have a

qualified Level II ATO. Training must be scheduled a minimum of three (3) weeks prior to traveling. N-NC/J2 provides the AOR threat update, which is available at https://www.noradnorthcom.smil.mil/CIFC/.

c. (U) AOR-Specific Training. Individuals traveling outside of CONUS in the USNORTHCOM AOR for either TDY/TAD or PCS must have received a specific AOR update within three months prior to travel. The AOR-specific update must include, at a minimum:

(1) (U) Current Terrorism Intelligence.

(a) (U) N-NC/J2 country-specific threat assessments are available on the NC/J34 classified website at https://www.noradnorthcom.smil.mil/j3/j34/.

(b) (U) Current country profiles and threat assessments are available on the Defense Intelligence Agency (DIA) classified website at http://www.dia.smil.mil/. (Select "Combating Terrorism" from the "Intelligence Subjects" menu, then select the country on the "Threat Assessments" pull-down menu.)

(c) (U) Additional threat information can be found on the N-NC/J2 classified website at http://j2web.northcom.smil.mil/.

(d) (U) Additional country-specific information can be found on the AFOSI home page. (Go to the "Quick Jump to Country" pull-down menu or to "NORTHCOM" under Commands.)

(e) (U) Finally, the Blue Lines, which are great summaries of unevaluated intelligence, can be found on the classified website http://www.afosi.af.smil.mil/.

(f) (U) Officials responsible for travelers who do not have a U.S. Secret clearance or access to terrorism intelligence should seek assistance through their force protection chain of command.

(2) (U) U.S. State Department Consular Information Sheets, Travel Warnings, and Public Announcements are available on an unclassified website at http://www.travel.state.gov/travel_warnings.html. DoD personnel and their eligible family members must comply with all State Department and USNORTHCOM prohibitions on travel. Commanders must counsel military personnel prior to approving any leaves to areas in which a State Department Public Announcement or Travel Warning is in effect. Commanders may disapprove travel of military personnel to any such location.

(3) (U) Location-specific Medical information.

(a) (U) Health threat briefings, pre-deployment briefings, and pre-deployment health screenings. (This applies to official travel only.) Commanders are responsible

for ensuring that health threat briefings; pre-deployment briefings and pre-deployment health screenings are conducted. All deploying personnel must be assessed and determined to be medically and psychologically fit for worldwide deployment. Immunization records must be screened and shots provided to protect against diseases in the deployment area. Depending on the mission, vulnerability assessment teams may include medical personnel with preventive medicine background to evaluate commands, personnel and facilities.

(b) (U) Medical Force Protection Requirements. All personnel must meet the published USNORTHCOM FP requirements and USNORTHCOM preventive medicine guidance available on the unclassified NIPRNet at https://www.noradnorthcom.mil/SG/. Health promotion, medical surveillance, and the prevention of illness, non-battle injury, and disease, including combat stress, must be integrated into the training of individual service members, into the training of military units, and into military exercises.

(c) (U) Additional Medical/Health Information. Additional information is available on the Armed Forces Medical Intelligence Center website at http://www.afmic.dia.smil.mil/intel/afmic/afmic.html. Information can also be found on the Centers for Disease Control unclassified website at http://www.cdc.gov/travel/.

(4) (U) If applicable, consult the classified TRANSCOM Port & Airfield Collaborative Environment (PACE) website at http://intelink.intel.scott.af.smil.mil/pace/index.cfm, which has information on port and airfield vulnerabilities.

d. (U) Level II Anti-Terrorism Officer (ATO). (This applies to official travel only.) Commanders of the Services, Task Forces, Joint Task Forces, Combined Task Forces, and deploying units down to the battalion, squadron, or ship level who are controlling, participating in, or supporting an operation or exercise must:

(1) (U) Appoint an ATO in writing to serve as the subject matter expert on AT matters. Assignment as the ATO may be a collateral or additional duty for the individual appointed. However, the ATO, as such, must report directly to the deployment commander. Smaller units, such as a company or flight, must also have an ATO if they deploy without their higher headquarters unless they are deploying as a subordinate element of a unit that with an ATO.

(2) (U) Ensure that the ATO is trained to employ methods for reducing the risk and mitigating the effects of a terrorist attack. The ATO must also be familiar with pre-deployment AT training requirements.

(3) (U) Ensure that the ATO has attended an approved Level II AT/FP course of instruction prior to the deployment. See DoDI 2000.16 for Level II AT/FP training requirements.

(4) (U) Complete and coordinate an AT plan for their operation through their unit ATO. See Tab B of this Appendix for an AT plan format for deployed units. Deploying units may also use the installation AT plan format found in Appendix 4 of *ref. f*. For travel to countries below FPCON Bravo, the first O-5 in the traveler's chain of command is responsible for approving the FP plan. For travel to countries at FPCON Bravo or higher, the first O-6 in the chain of command is responsible. For travel to areas with USNORTHCOM travel restrictions, the first O-7 in the chain of command is responsible. When applicable, a civilian senior executive service (SES) or equivalent exercising authority satisfies these requirements. A listing of current FPCONs in USNORTHCOM is available at https://www.noradnorthcom.smil.mil/j3/Operations/. (Click on "FPCON Levels and National Alert Status" under "Key References".)

(5) (U) Consider deploying the ATO early in the flow of deploying forces to execute AT/FP tasks that are requisite to the deployment, such as site survey or assessment and coordination of security requirements with the host nation.

(6) (U) Ensure proper AT/FP planning and execution. Note that units deploying in support of Incident Management missions are given specific guidance and planning assumptions that vary from those below. Specific planning factors vary with each operation, but the following represent basic issues to consider:

(a) (U) Use *ref m*; specifically, Table 2: Minimum Standoff Distances and Separation for Expeditionary and Temporary Structures, to determine if facilities either currently occupied or under consideration for occupancy by DoD personnel can adequately protect occupants against terrorist attack.

(b) (U) Do not assume that units already at the site or host-nation units will automatically provide AT/FP support. Likewise, do not assume the host nation will provide adequate security. All deployed DoD Elements should have an inherent security capability suitable for the mission and the type and level of threat at the deployment location. Deploying units may have to bring security forces or equipment and must take this into account when planning lift and support requirements. The deploying force must coordinate closely with USNORTHCOM to ensure all rapid determination of AT/FP requirements.

(c) (U) Factor AT/FP requirements into TPFDD planning to ensure that lift requirements and the timing the arrival of AT/FP do not impact adversely on mission capability.

e. (U) For all travel to locations outside the USNORTHCOM AOR, comply with the travel policies of the geographic combatant command to be visited.

(1) (U) These policies can be found in the FCG (*ref. cc*), as well as at the following links:

(a) (U) USEUCOM: http://www.eucom.smil.mil/ecsm/Predeployment/predeployment.html

(b) (U) USSOUTHCOM: http://scshqwb1.hq.southcom.smil.mil/cmd/default2.htm. Select "J3 - Operations" under "Community" on the left-hand side, then scroll down to the bottom-right and select "Pre-deployment Requirements" under "J371 AT/FP".

(c) (U) USPACOM: http://www2.hq.pacom.smil.mil/j3/j34/Default.asp?tab=2

(d) (U) USCENTCOM: http://recluse.centcom.smil.mil/ccj6/ccj6_d/ccj6dm/Publications/p310-1.htm (Select "55 - TRANSPORTATION AND TRAVEL".)

f. (U) The first General or Flag Officer or SES in the FP chain of command of the sponsoring organization must approve any conferences or similar gatherings in a foreign location or off of a secured DoD location in CONUS if the Terrorist Threat Level is Significant or High. For example, a USNORTHCOM conference planned for a country or a location outside of a secured CONUS DoD location where the Terrorist Threat Level is significant or high requires General or Flag Officer approval. Prior to scheduling in another country or off of a secured DoD location within CONUS, the approver must conduct an operational risk assessment, including coordination with the local ATO (if applicable) or American Embassy regional security officer. Commanders responsible for FP of such events must also approve them, with any disputes between the two approving authorities being resolved through their respective chains of command.

g. (U) The current list of DoD-approved air carriers can be found at the following unclassified link: https://amc.scott.af.mil/do/dob/alphalst.htm.

APPENDIX 5 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
IMPLEMENT SECURITY REQUIREMENTS AND FORCE PROTECTION CONDITIONS (FPCON) (U)

(U) References: *Base Order*.

1. (U) Situation. *Base Order*.

2. (U) Mission. *Base Order*.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) This critical task addresses the requirement to establish processes for the development and implementation of additional security measures that may exceed the parameters of the FPCON system based on mission specific requirements. However, FPCON setting and the processes for coordination are a critical task for USNORTHCOM and the DoD Elements in the USNORTHCOM AOR. Execution of this task has a significant impact on the operational missions of the DoD Elements in the USNORTHCOM AOR. This task is derived from the DoDI 2000.16 standards 1 - 3, 5, 11 - 14, 16, 17, and 20 and DoDD 2000.12 requirements 5.14.1, 5.14.2, 5.15.1, 5.17.1 - 5.17.13, and 5.17.16 - 5.17.18.

(2) (U) Commander, USNORTHCOM exercises TACON for DoD FP and assumes overall DoD AT Program and FP responsibility in the USNORTHCOM AOR IAW the UCP, DoDD 2000.12 and DoDI 2000.16 with the following modifications in regards to TACON (for FP) in CONUS: Commander, USNORTHCOM will not use his authority to move DoD personnel unless faced with a time-critical event involving potential loss of life, or personnel movement is required to prevent significant damage to mission-critical infrastructure. Commander, USNORTHCOM will notify SecDef immediately of such time-critical personnel movements. Commander, USNORTHCOM will seek SecDef approval of pending baseline FPCON changes no later than 24 hours prior to implementation or as soon as practicable if faced with a critical event.

(a) (U) Commander, USNORTHCOM is the sole recommender to the SecDef for the FPCON baseline for the USNORTHCOM AOR. When time allows, Commander, USNORTHCOM will request input regarding FPCON recommendations from the DoD Elements' AT offices and USDRs.

(b) (U) NC/J34 will provide FPCON recommendations to the USNORTHCOM Director of Operations (J3) and to the Commander, USNORTHCOM.

(c) (U) FPCON baseline decisions by the SecDef will be implemented through the DoD Elements in the USNORTHCOM AOR.

(d) (U) The DoD Elements retain authority to use increased FPCON measures above the baseline. A commander may raise the FPCON above the USNORTHCOM established baseline and return the FPCON to the baseline based on the threat. However, commanders may not lower the FPCON below the USNORTHCOM established baseline without prior coordination and approval from Commander, USNORTHCOM. Commanders will report within 4 hours increases above the baseline through their chain of command to the NCOC and NC/J34, to include reason for the increase.

(3) (U) FPCON Settings. Specific measures associated with the various FPCON levels as well as shipboard measures are listed in Appendix 3 of ref. f. The terminology, definitions, and specific recommended security measures are designed to facilitate inter-service coordination and support for the combating terrorism efforts of the DoD Elements.

(a) (U) An AT plan with a complete listing of site-specific AT measures, linked to a FPCON, will be classified, as a minimum, CONFIDENTIAL. When separated from the AT Plan, specific AT measures and FPCONs remain FOR OFFICIAL USE ONLY.

(b) (U) Implementation of FPCONs does not come without adverse effects on day-to-day operations; the additional costs can be measured and described both quantitatively and qualitatively. The FPCON system acknowledges cost as a significant factor bearing on the selection and maintenance of FPCONs. FPCONs ALPHA and BRAVO include measures that can be sustained for extended periods, consistent with the terrorist threat.

(c) (U) The declaration of a FPCON constitutes raising the security posture of an activity above a "no threat" status.

(d) (U) USNORTHCOM will list all measures from higher FPCONs as applicable when describing and reporting FPCONs that incorporate additional AT measures above the established baseline. DoD Elements that set FPCON will list additional AT measures from a higher FPCON and report this accordingly in FPCON Change Reports or Monthly FP Updates to USNORTHCOM. Report will include a listing of measures used from a higher FPCON (e.g., FPCON Alpha with Bravo 3, 5 & Charlie 4).

(e) (U) Escalating the FPCON should enhance capabilities, mitigate the threat, and send a clear signal of increased readiness. Random implementation of a variety of security measures should be included in all aspects of AT planning to produce a discernable element of unpredictability in procedures. Extended periods of elevated FPCON will result in diminishing returns, as increased measures become normal operating procedures. Therefore, each commander will make Random Antiterrorism Measures (RAMs) an integral part of his/her AT plan. Terrorist pre-attack surveillance

should be assumed and emphasis given to detecting such activity at every stage of security alert.

b. (U) Tasks.

(1) (U) Commanders declare FPCON levels for forces or installations subject to their command authority. This ensures the execution of the most appropriate response to an assessed threat for a specific area, base, unit, or command. DoD Elements and personnel located in non-DoD controlled facilities under the jurisdiction of another agency or entity (GSA leased non-delegated facilities, etc.) will follow the GSA Security Alert System imposed by the Department of Homeland Security.

(2) (U) Commanders and their staffs will examine the threat, physical security, operational environment, terrorist attack consequences, and mission vulnerabilities in the context of specific DoD activities and the declared FPCON. When factors are combined and the collective threat exceeds the ability of the current physical security system (barriers, surveillance and detection systems, security forces, and dedicated response forces) to provide the level of asset protection required, then implementation of higher FPCONs or additional measures is appropriate.

(3) (U) The FPCON system allows Commanders flexibility and adaptability in developing and implementing AT measures that are more stringent than those mandated by higher authorities whenever FPCONs are invoked.

(4) (U) Each set of FPCON measures is the 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.

(5) (U) Authorities directing implementation may add measures from higher FPCONs at their discretion. Commanders may implement additional FPCON measures on their own authority, develop additional measures specifically tailored for site-specific security concerns, or declare a higher FPCON for their AOR/installation.

(6) (U) Normally, the FPCON posture at any given location will be unclassified.

(7) (U) Commanders will publish guidance outlining procedures for implementing the FPCON system, which at a minimum requires subordinate commands to:

(a) (U) Notify the chain of command and any other installations/commands in the area of any FPCON changes.

(b) (U) Develop local preplanned measures and coordinated US/Host Nation military and police security measures commensurate with the requirements of each FPCON level.

(c) (U) Identify local critical and/or mission essential areas, infrastructure and activities, high-risk personnel and off-installation areas frequented by DoD personnel; and develop pre-planned protective measures for these potential terrorist targets consistent with each FPCON level.

(d) (U) Implement USNORTHCOM-directed FPCON level changes and additional measures, as appropriate, immediately upon receipt of notification.

(8) (U) It is essential for Commanders to implement formal analytical processes that result in a set of AOR or locality-specific terrorist threat indicators and warnings for use when transitioning from lower to higher FPCONs.

(9) (U) All Commanders will ensure that their subordinates fully understand FPCON declaration procedures and FPCON measures. Such processes and measures should be harmonized to the maximum degree possible, taking fully into account differences in threat, vulnerability, criticality, and risk of resources requiring protection.

(10) (U) To enhance the overall effectiveness of a given FPCON, Unit Commanders will develop and implement a RAM program as an integral part of their AT Program. Advantages of implementing RAMs include, but are not limited to:

(a) (U) Variation in security routines makes it more difficult for terrorists to target important assets, build detailed descriptions of significant routines, or predict activities by a specific asset or within a targeted facility or installation.

(b) (U) Increased AT awareness for DoD personnel, their family members, visitors, and neighbors.

(c) (U) Increased alertness among law enforcement, security, and base or facility personnel.

(d) (U) Reduced adverse operational effects and unplanned economic costs when enhanced AT measures must be maintained for extended periods.

c. (U) Coordinating Instructions.

(1) (U) FPCON Measures. The FPCON measures defined in Appendix 3 (DoD FPCON System) of *ref. f* are not all inclusive and some may not be practical for a specific situation. Each unit's AT Plan will incorporate existing FPCON measures and any additional measures (location specific) that enhance the security of unit personnel, families, and facilities.

(2) (U) Reporting Changes in FPCON Levels. Supporting commands and USDRs will report any changes in FPCON status up the chain of command to the NCOC and NC/J34 IAW Appendix 1 to Annex C and Annex R, Reports.

(3) (U) FPCON Waivers.

(a) (U) If it is determined that certain FPCON measures are inappropriate for current operations, or for proper threat mitigation, Commanders or DoD civilians exercising equivalent authority may request a waiver. The first General/Flag Officer exercising TACON (for FP) or DoD civilian member of the Senior Executive Service (SES) exercising equivalent authority in the chain of command is the approval authority for waiver of specific FPCON measures. Commander, USNORTHCOM, his deputy, or DoD civilians exercising equivalent authority may delegate this authority below the general/flag officer level on a case-by-case basis. Any senior military Commander having TACON (for FP) or DoD civilian member of the SES exercising equivalent authority may withdraw first General/Flag Officer or DoD civilian authority and retain this authority, at his or her discretion. Waiver authority for specific FPCON measures directed by a higher echelon (above first General/Flag Officer or DoD civilian member of the SES) rests with the military Commander or DoD civilian exercising equivalent authority directing their execution. Nothing in this waiver process is intended to diminish the authority or responsibility of military Commanders or DoD civilians exercising equivalent authority, senior to the waiver authority, to exercise oversight of FPCON and RAMs program execution.

1. (U) To ensure a consistent FP posture is maintained, tenants on CONUS installations and facilities shall coordinate waiver actions with the host installation before submitting them to their chain of command.

2. (U) All waiver requests shall be directed to the waiver authority. Information copies shall be sent to NC/J34, Major/Fleet Command's operations center, Service operations center or DoD civilian operations center as applicable.

3. (U) Approved waivers, to include mitigating measures or actions, must be forwarded to NC/J34, Service, Combatant Command, Major/Fleet Command, or DoD civilian equivalent command-level recipients within 24 hours of approval.

Tabs:

A. Traveler FPCON Procedures (U)
B. Deployed Unit FPCON Procedures (U)

APPENDIX 6 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
AT VULNERABILITY AND PROGRAM ASSESSMENTS (U)

(U) References: *Base Order*.

1. (U) Situation. *Base Order*.

2. (U) Mission. *Base Order*.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) Purpose. The Vulnerability Assessment (VA) and AT Program Review (PR) processes and resulting database provide a common operational picture to support risk management decisions in the USNORTHCOM AOR. The specific standards from DoDI 2000.16 (*ref. d*) supporting this critical task are: 2, 3, 5, 15, 20, 26, 27, 29 and 30. The supporting DoDD 2000.12 (*ref. c*) requirements are: 5.14.1, 5.14.5, 5.15.2.2, 5.17.1, 5.17.2, 5.17.4 5.17.8, 5.17.9, and 5.17.17. In addition to the Assessment and Review processes, the VA database serves as the centerpiece for assessing the AT posture and vulnerabilities within the USNORTHCOM AOR. The AT VA program, when integrated with CIP, the CBRNE program, and Information Operations (IO) VA programs, will provide a comprehensive picture. When the VA programs are synchronized with current information/intelligence, it will facilitate timely and accurate decisions regarding FP.

(2) (U) All DoD Elements and personnel under the AT responsibility of Commander, USNORTHCOM will be assessed to determine their vulnerabilities using the guidelines and criteria stipulated in Tab A of this Appendix. This criteria forms the fundamental basis by which Assessments are conducted in the USNORTHCOM AOR. Standards promulgated by the Services, other Combatant Commands, Defense Agencies and DoD Field Activities are considered complementary to the core criteria noted. In the event of a conflict between Service, Defense Agency or DoD Field Activity or other Combatant Command standards, the USNORTHCOM standards will override the conflicting command's standards IAW *refs. c and d*.

(3) (U) Per DoDI 2000.16, Standard 20, Commanders at all levels will conduct annual internal AT Program reviews of their respective AT Program as well as an annual review of the AT Program of their immediate subordinates in the chain of command. Organizations (USNORTHCOM, DTRA, PFPA, etc.) conducting AT Program Reviews within USNORTHCOM will utilize the Joint Staff AT Program Assessment Benchmarks for the Services, Combatant Commands, Defense Agencies and DoD Field Activities as the baseline guidance when conducting AT Program Reviews. These AT Program reviews will be designed to determine compliance with DoD and USNORTHCOM AT standards.

(4) (U) In addition to Program Reviews, Service POCs, Defense Agencies and DoD Field Activities, Combatant Commands and Commanders will conduct VAs using the DTRA JSIVA guidelines that support the requirements delineated in Standard 26 (*ref. d*). The DoD Element-designated AT representative responsible for addressing USNORTHCOM AT issues will also arrange for triennial higher headquarters (HHQ) VAs to satisfy the frequency criteria specified in Standard 26. The JSIVA benchmarks will be the minimum and mandatory standards for the USNORTHCOM AOR for assessments at all levels (JSIVAs, HHQs Assessments, USNORTHCOM Assessments, Local VAs). After coordinating with the DoD Elements' designated POC for VA oversight, USNORTHCOM will submit all JSIVA requirements to the Joint Staff for the USNORTHCOM AOR. The DoD Elements will identify JSIVA requirements to NC/J34 NLT 15 June of the calendar year preceding the calendar year assessment cycle. In turn, after collating, prioritizing and vetting the Service and Agency requirements, NC/J34 will submit USNORTHCOM's total JSIVA requirement to the Joint Staff on or about 1 July (or by the suspense date specifically required by the Joint Staff).

(5) (U) Vulnerability Assessments. USNORTHCOM will use a tiered approach to VAs. The three tiers are as follows:

(a) (U) VAs (Tier 1). To standardize the VA process for coherency throughout the Command, USNORTHCOM has adopted the DTRA JSIVA guidelines (Tab A), dated 1 March 2002 as the required basis by which local level or higher headquarters commands conduct VAs. DoD Elements will submit requests for modification of the JSIVA guidelines to NC/J34. For installations and facilities that normally do not meet the threshold requirements for a VA stipulated in *ref. d*, DoD Elements will arrange for a VA (with the assistance of the DoD Elements, the DoD Elements' AT designated representative, and/or USNORTHCOM as required when the installation or facility is deemed mission critical by DoD, USNORTHCOM, or the DoD Elements. Vulnerabilities will be determined using the DIA Threat Assessment, the installation's Local Threat Assessment (LTA), Criticality Assessment and Design Basis Threat (DBT), which is derived from the LTA.

1. (U) VAs will also be conducted by USNORTHCOM in a "Combined" format with the Canadian Armed Forces (at Canadian installations which retain U.S. personnel and/or a U.S. interest); to support National Special Security Events (NSSEs) when directed by USNORTHCOM; and by the DoD Elements to support high-visibility/high-use non-DoD facilities (ports and airfields). The DoD Elements will conduct Integrated Vulnerability Assessments (IVAs) as required to support movement between DoD facilities, APOE/SPOEs and civilian infrastructure supporting DoD operations.

2. (U) HHQs Assessment Teams. The following are some of the Higher Headquarters (HHQs) teams available to conduct assessments/program reviews: DTRA/JSIVA teams, Service/Agency/Activity teams (AFVAT, NIVA, DAFPAT), intermediate HQ teams (e.g. MAJCOMs, MACOMs, etc.), USNORTHCOM and the Joint Staff (for Program Reviews only). The JSIVA purpose and methodology is discussed in

more detail below. NC/J34 will monitor and record (based on data provided in the LRC) the type of VA (JSIVA, Service Headquarters, MAJCOM/MACOM, etc.) that each assigned organization receives.

(b) (U) Security Assessments (Tier 2). Consistent with the threat, USNORTHCOM will use Security Assessments (Tab B) to assess the vulnerability of non-DoD facilities (ports and airfields) used infrequently by DoD personnel. Security Assessments are authorized when the DIA Threat Level is Medium or Low and DoD aircraft, ships and/or ground contingents remain overnight (RON) and entail more than 100 personnel. The "Security Assessment" will also serve as the basis for units and organizations within USNORTHCOM that do not ordinarily meet the threshold requirements for VAs stipulated in *ref. d*. Typically, this applies to satellite units, geographically separated units (GSU), etc. consisting of less than 300 DoD-assigned personnel. Execution of the Security Assessment is the responsibility of the unit's headquarters and/or host/support organization. The satellite/GSU, etc. will conduct a self-assessment at least annually with the parent/HQs unit accomplishing the assessment on a triennial basis. DoD Elements will submit requests for modification of the security assessment guidelines to NC/J34. Subject to unique circumstances, modifications are guidelines that are "in addition to" vice "replacement" of USNORTHCOM Security benchmarks. The USNORTHCOM Port checklist is Enclosure 1 to Tab B. The USNORTHCOM Airfield checklist is Enclosure 2 to Tab B. The USNORTHCOM In-transit checklist is Enclosure 3 to Tab B.

(c) (U) Virtual Assessments (Tier 3). Consistent with the threat, USNORTHCOM will use virtual assessments to assess the vulnerability of non-DoD facilities or locations without a DoD presence that will only be used in contingency/emergency situations and/or for a short duration (less than 24 hours and do not RON) and when transited by limited numbers of DoD personnel (100 or less). Virtual assessments are authorized when the DIA Threat level is Low. Virtual assessments will contain as much current information available as possible regarding terrorist and criminal threat/capability at that location.

(6) (U) Required Frequency.

(a) (U) Program reviews of USNORTHCOM subordinate Headquarters will be conducted annually. Commanders will conduct VAs at least annually for facilities, installations, and operating areas within their AOR to include tenant organizations assigned to an installation.

(b)(U) Higher Headquarters (HHQs) VA. Installations must receive a HHQs level AT VA every 36 months. The HHQs VA satisfies the annual local VA requirement for that year. To preclude a "parochial", DoD Element only, singularly focused view on assessments, the DoD Elements' designated AT representative responsible for scheduling HHQ assessments will ensure JSIVAs are scheduled for installations as part of the triennial requirement.

b. (U) Tasks.

(1) (U) Commanders. Commanders will ensure they integrate/coordinate assigned tenant organizations into their respective AT Programs, and will ensure the tenant's inclusion as part of the host's installation VA.

(2) (U) DoD Elements. The DoD Elements (and/or their designated AT representative) will provide HHQs VA long-range calendars (LRCs) to NC/J3 to facilitate USNORTHCOM retaining visibility on scheduling and tracking of vulnerability assessments in its area of responsibility. For scheduling, the LRCs will encompass detailed information on the next immediate assessment year and tentative scheduling for years two through ten which detail projected local and HHQs/USNORTHCOM Assessments/JSIVAs. The calendar data will also include the dates of previous HHQs VAs/DTRA JSIVAs/USNORTHCOM Assessments and the specific assessment agency which conducted the previous assessments. The LRC will be updated annually. NC/J34 will coordinate with the DoD Elements and DTRA to ensure USNORTHCOM is in receipt of the schedule before the start of the annual Assessment scheduling cycle. This transaction will take place in June/July of the year prior to the Assessment year. The DoD Elements' AT designated representative and PFPA will have the LRC to NC/J34 NLT 15 June. A copy of the LRC will be forwarded to the Joint Staff J34 to facilitate scheduling.

(3) (U) USNORTHCOM will establish the annual Program Review schedule for the DoD Elements NLT 1 July preceding the execution year.

(4) (U) Assessment Requirements.

(a) (U) VAs. The basis for any VA conducted within the USNORTHCOM AOR is the DTRA JSIVA guidelines. The five core areas of an assessment are: Terrorist Options, Security Operations, Structural Engineering, Infrastructure Engineering, and Operational Readiness. Based on site/unit unique assets, the VA may also include port, DoDEA schools, WMD, Forward Operating Locations, and Interim Defense Agency Headquarters assessments.

(b) (U) AT Program Assessments. Commanders at all levels will review and document the results of the review of the AT Program and Plan of their immediate subordinate in the chain of command at least annually. NC/J34 will ensure on-site program assessments of DoD Elements annually. At the installation level, the AT Plan will address the following key elements. These key elements must be integrated into and/or support a comprehensive AT plan. Thus, stand-alone documents (e.g., SOPs, local regulations, or OPORDs that articulate requirements for these key elements) will be replicated in and/or referenced in the AT Plan. The AT Plan can also be a part of a stand-alone document:

1. (U) Local Threat Assessment.

2. (U) Design Basis Threat.

3. (U) Criticality Assessment.

4. (U) Vulnerability Assessment (*see ref. d, Standard 26*).

5. (U) Risk Assessment.

6. (U) Risk Management.

7. (U) Terrorist Incident Response measures.

8. (U) Terrorist Incident Management measures.

(c) (U) Non-DoD Ports and Airfields.

1. (U) Requirement. Assessments are required for use of CONUS ports and airfields in support of routine and force projection operations. The DoD Elements are responsible for ensuring execution of these assessments. The assessments may be Tier 1, 2 or 3 depending on the level of threat, the number of DoD Elements and personnel involved and frequency of use.

2. (U) Waivers. The first General Officer in the chain of command may waive these requirements for deployments and/or visits to DoD-controlled locations such as existing military installations or ships afloat. On-scene pre-deployment assessments of locations where the Terrorism Threat level is Low or Moderate will be at the discretion of the responsible commander unless otherwise specified. Non-DoD controlled locations will be assessed (minimum Tier 3) prior to use in accordance with this annex.

3. (U) Responsibility for Airfield Assessments

a. (U) Non-DoD Controlled Airfields.

a) (U) The Service/Agency deploying aircraft/providing airlift capability is responsible for the execution of assessments on all non-DoD airfields in the USNORTHCOM AOR. DoD Elements should coordinate with USTRANSCOM for availability of current USTRANSCOM/AMC assessments.

b) (U) Multiple Airfield Users. To avoid duplication of effort when two or more Services/Agencies use a non-Service specific location, responsibility for conducting the assessment will generally follow in the order shown below for the Services in question:

1) (U) Fixed Wing Locations: Air Force, Navy, Army, USSOCOM, and Marine Corps.

2) (U) Rotary Wing Locations: Army, Air Force, USSOCOM, Navy, and Marine Corps.

b. (U) Disagreements. Disagreements over assessment responsibility, which cannot be resolved by HQ USAF, will be addressed to NC/J34 for resolution.

4. (U) Responsibility for Port Assessments.

a. (U) The Service/Agency deploying vessels/providing sealift capability is responsible ensuring execution of assessments on all non-DoD ports in the USNORTHCOM AOR. DoD Elements should coordinate with USTRANSCOM for availability of current USTRANSCOM assessments. The U.S. Coast Guard Captain of the Port should also be contacted for his/her assessment.

(5) (U) USNORTHCOM VA Tasks.

(a) (U) USNORTHCOM conducts “spot assessments” within the USNORTHCOM AOR when requested by Commander, USNORTHCOM, when the current threat and mission criticality warrant and/or when the Services or agencies. NC/J34 will endeavor to conduct one spot assessment per quarter, generally corresponding to one spot assessment per Service per year. With a mature VA data base (via the Core Vulnerability Assessment Program [CVAMP]), spot assessment selection will evaluate installations with chronic repeat procedural vulnerabilities and demonstrated inaction on mitigation plans. USNORTHCOM will normally execute spot assessments no earlier than 6 months after the completion of a VA or Security Assessment. USNORTHCOM will forward the results of the spot assessments via the USNORTHCOM Chief of Staff to the DoD Elements.

(b) (U) USNORTHCOM conducts VAs for National Special Security Events (NSSE) and Special Security Events (SSE).

1. (U) As the supported Commander, Commander, USNORTHCOM executes TACON (for FP) for those DoD forces mobilized/deployed to support NSSEs/SSEs. By their nature, NSSEs/SSEs are lucrative targets and potential Mass Casualty venues for terrorist attacks.

2. (U) USNORTHCOM intends to reduce the risk to DoD forces at NSSEs/SSEs through two mechanisms. The first is to use existing VAs generated by the Local installation, HHQs, supporting DoD Elements and PAs. The second is to conduct unilateral VAs when required or requested. While not conducted exclusive of the event itself, VAs conducted by USNORTHCOM, subordinate DoD Commands will be principally DoD-focused. The prime intent is to mitigate risk by assessing

vulnerabilities to DoD personnel at fixed facilities (billeting, command posts, etc), operational sites, lines of communication (ground, sea, air and supply routes), and sustainment nodes (messing, fuel, transportation, etc).

3. (U) The operational timelines for planning and executing NSSEs/SSEs can generally preclude extensive pre-event AT planning at the JTF level. Early identification of FP issues and assumptions necessary for effective planning are critical to effective risk mitigation during the event. NC/J34, as part of the overall USNORTHCOM strategic planning effort, will conduct initial planning and coordination with the for AT requirements. After identifying the requirements, USNORTHCOM will task the appropriate DoD Element to conduct assessments. HQ USNORTHCOM will provide a Level II ATO with JTF-N when they are a supporting Headquarters. Upon completion, the tasked DoD Element will forward the assessment findings and recommendations to NC/J34 for macro analysis, red teaming and strategic level VA development. Emphasis on the identification of mitigation resource requirements is particularly critical. NC/J34 will provide appropriate input to the OPORD and/or EXORD. NC/J34 will provide the entire VA packet to the JTF Commander or subordinate DoD Headquarters. Tab D (NSSE Planning Process) to this appendix provides a general six-month timeline from notification for AT planning activities in support of NSSEs/SSEs. In the event there is less than six months from notification to execution, the timeline will be compressed as appropriate. The JTF/Senior DoD Commander should conduct a risk assessment by phase of the operation. A sample risk assessment (Figure C-6-1) and Risk Assessment Worksheet (Figure C-6-2) are provided below. General Officer notification of risk acceptance or assistance is required when there are Extremely High levels of residual risk.

			HAZARD PROBABILITY				
			Frequent	Likely	Occasional	Seldom	Unlikely
			A	B	C	D	E
EFFECTS	Catastrophic	I	Extreme		High		Moderate
	Critical	II	Extreme	High		Moderate	Low
	Marginal	III	High	Moderate		Low	
	Negligible	IV	Moderate	Low			

Figure C-6-1

RISK ASSESSMENT WORKSHEET								
Activity or Exercise Name:	Organization:	Date:	Prepared By:	Page 1 of				
HAZARDS	Mishap-Prob	Effect	Risk Level	Controls Implemented	Implemented By	Residual -Prob	Residual - Effect	Residual Risk Level

Figure C-6-2

4. (U) The VA associated with NSSE is ultimately focused to produce the Threat and VA Product (TVAP); it is generated by NC/J34 to provide information relative to the command's planning for NSSEs and SSEs. The N-NC/J2 and CIFA-West provide threat assessments, DPO-MA provides a CIP sector analysis, and NC/J34 provides the criticality, vulnerability and risk assessments. The purpose of the TVAP is to identify overall risk to DoD forces supporting a designated event for Commander, USNORTHCOM and designated JTF Commanders. The development of the TVAP is critical to the production of pertinent, specific FP instructions for inclusion in the Command's EXORDs. Information contained in the TVAP includes: Event Threat Assessment, Criticality Assessment, VA, Risk Assessment, Mitigation Strategies Residual Risk Assessment and FP Instructions.

(c) (U) USNORTHCOM conducts Combined (Canada-US) VAs. Commander, USNORTHCOM retains FP responsibility for all DoD personnel not under the direct responsibility of a COM. To assist the Commander in executing their responsibility to assess and review the AT/FP Programs of all Commander-assigned military forces and/or activities, the Combined Vulnerability Assessment Team (CVAT) is employed. CVATs execute a comprehensive VA program which assesses, analyzes and provides options to mitigate and/or eliminate threats to DoD/Canadian Force (CF) personnel, resources, infrastructure, information and equipment across the threat spectrum within the CANUS AOR in order to ensure mission accomplishment. The CVAT is the venue by which Commander, USNORTHCOM ensures lower-level AT Programs receive a

HHQs VA at least once every three years mandated by DoD directives and instructions. CVATs are conducted at locations where DoD and CF resources are collocated and with the concurrence of the local commander. As with all VAs conducted within the USNORTHCOM AOR, the JSIVA methodology is the basis by which VAs are conducted by the CVAT. That is, it approximates the same team subject matter expertise, length of assessment and briefing/reporting criteria as exercised by DTRA when conducting JSIVAs. Additionally, installations assessed by the CVATs are CAF installations. Accordingly, assessment benchmarks utilized are not "pure" DTRA benchmarks, but a close modified approximation and derivative thereof. The intent of the CVAT program is further expansion to conduct combined assessments with DHS, NGB, and Mexico.

(d) (U) USNORTHCOM participates on HHQs VAs conducted within the USNORTHCOM AOR as observers. The purpose is to: ensure uniformity in application of the USNORTHCOM AT Program and its adjunct assessment process; provide findings to the specific HHQs Assessment Team conducting the assessment (relative to methodology and compliance with DoD and USNORTHCOM assessment objectives); and provide the basis for generating action plans for VA process improvement. NC/J34 endeavors to observe one HHQs VA conducted by the DoD Elements' subordinate HHQs team per year as well as one JSIVA per Service/Agency per year. Taken together, NC/J34 observes one HHQs VA and/or JSIVA per month.

(e) (U) USNORTHCOM conducts "Red Team" operations as an additional option for assessing vulnerabilities at select installations and against specific targets. Red Teams (opposing forces) evaluate potential vulnerabilities against emerging terrorist capabilities by conducting operations which replicate identified "threat" forces. USNORTHCOM Red Team options include a tiered approach which provides options to tailor activities based on requirements. Red Team operations emulate threat elements against DoD facilities and will be initiated by an installation, or DoD Element request.

(6) (U) JSIVAs/HHQs VAs/USNORTHCOM Assessments.

(a) (U) The Chairman of the Joint Chiefs of Staff (CJCS), as the principal advisor to the SecDef for AT issues, is tasked to assess DoD Element policies and programs. To accomplish this task, the CJCS sponsors the JSIVA program through the Joint Staff J34, Deputy Director for Antiterrorism/Homeland Defense (DDAT/HD). (As the annual number of available JSIVAs far exceed requirement, Commanders must fill the gap with HHQs Assessments/USNORTHCOM Assessments; they do so by emulating the DTRA JSIVA process.) Combatant Commanders, Services, Defense Agencies and DoD Field Activities are required by DoDI 2000.16 to assess their installations triennially with a HHQs Assessment and AT programs annually. Combatant Commanders, Services, Defense Agencies and DoD Field Activities can request JSIVAs to meet their assessment responsibilities.

(b) (U) In addition to the core JSIVA allocations, specially tailored JSIVAs are performed when requested by Combatant Commanders, as contingencies require. The earlier they are identified (preferably within the scheduling window) the better chance in

getting the requirement fulfilled efficiently. In response to the USS Cole bombing and Government Accountability Office (GAO) report findings, the scope of the JSIVA process was expanded to include HHQs, strategic sea and airports, and JCS exercises.

(c) (U) Methodology. Three phases of the JSIVA (and suggested format for HHQs Assessments, USNORTHCOM Assessments):

1. (U) PHASE ONE (Visit Prep). Installations are contacted approximately 75 days before the visit. A request is made for points of contact, mission statement, local threat assessment, and copies of AT related plans. During this phase, installation Commanders provide the JSIVA team with actions taken to reduce previous JSIVA/HHQs/USNORTHCOM team identified vulnerabilities.

2. (U) PHASE TWO (Site Assessment). The assessment begins with an installation tour, usually the day before the in-brief, and installation mission brief on day one. The visit culminates on day five with an out-brief provided to the installation Commander and his/her key staff.

a. (U) During the weeklong assessment, the JSIVA/HHQs/USNORTHCOM team reviews site-specific plans, programs and procedures. They assess tactical warning actions, FPCON implementation, physical security systems, guard-force procedures, and incident response and IM capabilities.

b. (U) Members of the team normally provide tutorials to their respective installation counterparts during the week.

3. (U) PHASE THREE (Post-Visit). After the visit, a formal report is written and provided to the installation Commander within 60 days.

NOTE: Regarding the methodology by “phase” noted above for JSIVAs, HHQs Assessment/USNORTHCOM Teams are encouraged to following the same “phasing” to the extent feasible.

(e) (U) Once this report is received, the installation Commander must report to the first General/Flag Officer in the chain of command within 30 days (of receipt of the report) on actions taken on identified vulnerabilities.

(7) (U) Vulnerability Assessment Reporting Requirements. *Annex R, Reports*.

(8) (U) Core Vulnerability Assessment Management Program (CVAMP). CVAMP is a database that gives ATOs at all levels the ability to manage information regarding installation-level vulnerabilities within USNORTHCOM. CVAMP is under revision to incorporate IO, CBRNE and CIP assessment results, as well as AT.

(a) (U) Functions. CVAMP provides:

1. (U) Required VAs for each installation, base and facility.

2. (U) Vulnerability Listing/Status. Listing of the vulnerabilities of an activity or installation and the current status of repair or redress of those vulnerabilities.

3. (U) Trend Analysis. Trend analysis is a record of FP efforts and improvements over time.

4. (U) Documentation. Documents a Commander's risk assessment decision for each identified vulnerability.

5. (U) Tracking System. Tracks the status of known vulnerabilities until mitigated.

6. (U) Ability to prioritize AT/FP resource requirements and input into the PPBE process.

7. (U) Commanders a vehicle to identify requirements to the responsible chain of command.

8. (U) A ready reference to track the status of installations and activities by FPCON and/or Terrorism Threat Level.

9. (U) Provides a database to document Standard 26 VA findings, both at HHQs and locally.

10. (U) Ability to identify and prioritize AT emergent/emergency requirements into the CbT RIF portion of CVAMP.

(b) (U) Requirements.

1. (U) DoD Elements Initial Data Entry. Within 30 days of receiving a report or completing an assessment, Services/designated AT representatives for the Services will ensure vulnerability data has been registered into the CVAMP by the installation ATO.

2. (U) Quarterly Updates. The DoD Element and Combatant Commands will ensure quarterly updates of their portion of the database are made.

3. (U) Installations. Updates will also be provided when completing a follow-up assessment of an installation/facility.

4. (U) Units and installations make corrections and/or address shortcomings from previous assessments.

NOTE: CVAMP is a SIPRNet application. While the program itself is unclassified, the data and compilations the program assembles can be classified up to SECRET. CVAMP data may not be transferred off the SIPRNet for any reason. CVAMP can be accessed at http://204.20.43.31/vamp.

(c) (U) CVAMP Concept Of Operations.

1. (U) The NC/J34 monitors the CVAMP and is responsible for coordination with the Joint Staff in the design, integration, and upgrading of the CVAMP system. NC/J34 is responsible for assisting the Joint Staff in the design and upgrade of this system, provides read/write permissions as appropriate and conducts training as needed. USNORTHCOM has recommended updates to CVAMP to support increased fidelity and analysis capability. Until these upgrades become effective (date TBD) USNORTHCOM requires electronic copies of VAs within 30 days of receipt of report.

2. (U) DoD Elements' AT offices monitor the CVAMP for accuracy and timely input of data inputted by the installation ATOs. Additionally, the DoD Elements use the data to develop AT funding priorities.

3. (U) Installation ATOs administer the CVAMP by entering, editing, and maintaining accuracy of data. ATOs must validate the accuracy of CVAMP data monthly and edit/update the CVAMP:

a. (U) Upon completion of an assessment by either local, JSIVA, USNORTHCOM or HHQ installations must enter known vulnerabilities (versus observation/concerns, observations/positives) identified during VAs NLT 10 duty days after the installation Commander out-brief. Installations must input all other observations/concerns and observations/positives identified by JSIVAs, HHQs or local VA teams NLT 30 days following receipt of the written report (normally received within 60 days of completion of the VA).

b. (U) Whenever the status of a vulnerability changes (e.g. vulnerability eliminated, project design status change or project funded).

c. (U) As soon as possible after changing the FPCON.

4. (U) CVAMP access is controlled and limited to a "need to know" basis. Individuals with a need to establish a CVAMP account must submit a request to their DoD Element AT office. Individuals not assigned to a specific DoD Element should contact NC/J34 directly.

Tabs:

A DTRA JSIVA Benchmarks (U)

B Security Assessment Checklists (U)
Enclosure 1: Port Checklist (U)
Enclosure 2: Airfield Checklist (U)
Enclosure 3: In-transit Checklist (U)
C Joint Staff Antiterrorism Program Assessment Benchmarks For Combatant Commands, Defense Agencies and Field Activities (U)

TAB A TO APPENDIX 6 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
DTRA JSIVA BENCHMARKS (U)

1. (U) Use of the DTRA AT VA Team Guidelines (JSIVA) Program, 1 March 2002, is compulsory for all VAs conducted within the USNORTHCOM AOR.

2. (U) This document may be accessed from USNORTHCOM website: https://www.noradnorthcom.smil.mil/j3/j34 under the Documents, Publications and Presentations section.

TAB C TO APPENDIX 6 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
JOINT STAFF ANTITERRORISM PROGRAM ASSESSMENT BENCHMARKS FOR COMBATANT COMMANDS, DEFENSE AGENCIES AND FIELD ACTIVITIES (U)

1. (U) Use of the USNORTHCOM Antiterrorism Program Assessment Benchmarks for Services, Defense Agencies and Field Activities is compulsory when conducting AT Program Reviews within the USNORTHCOM AOR. The Benchmarks are a derivative, expanded version of the Joint Staff Antiterrorism Program Assessment Benchmarks for Combatant Commands, Defense Agencies, and Field Activities.

2. (U) This document may be accessed from the USNORTHCOM website: https://www.noradnorthcom.smil.mil/j3/j34 under the Documents, Publications and Presentations section.

APPENDIX 7 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
AT RESOURCING (U)

(U) References: *Base Order*.

a. (U) CJCS Instruction 5261.01C, Combating Terrorism Readiness Initiatives Fund, April 1 2003.

b. (U) DoD Directive 7045.14, The Planning, Programming and Budgeting System (PPBS), 21 Nov 03.

c. (U) Management Initiative Directive (MID) 913, Implementation of a 2-Year Planning, Programming, Budgeting, and Execution Process.

d. (U) CJCSI 8501.01, Chairman of the Joint Chiefs of Staff, Commander in Chiefs of the Combatant Commands, and Joint Staff Participation in the Planning, Programming, and Budgeting System.

1. (U) Situation. *Base Order*.

2. (U) Mission. *Base Order*.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) This critical task is derived from USNORTHCOM's responsibilities to: a) advocate for AT requirements of the DoD Elements in the Planning, Programming, Budgeting, and Execution (PPBE) process; and, b) to manage the Combating Terrorism Readiness Initiatives Fund (CbT RIF) program for the USNORTHCOM AOR. As detailed previously in this OPORD, USNORTHCOM considers AT resourcing part of the risk management process under its FP mission. The USNORTHCOM FP mission supports or enables the mission planning and execution of the other Combatant Commands. Therefore, an integrated and efficient resource process for the USNORTHCOM AOR is essential to enable the FP mission and AT program.

(2) (U) The central element within the USNORTHCOM comprehensive AT resource process for the USNORTHCOM AOR is an integrated risk management approach. This approach factors in critical capabilities and vulnerabilities in the context of a mission planning/execution timeline, and threat capabilities/intentions. The resultant risk management determinations thus provide operational mission impact substantiation for resource requests, and enable resource strategy adaptation. Since DoD risk management remains an evolving construct, the USNORTHCOM AT resource process directs the use of risk management within all theater resource processes rather than mandating use of a specific risk management methodology or approach.

(3) (U) An effective AT program requires a well-defined process to identify and document and monitor resource requirements. In general, the key elements of the process include prioritizing the requirements, identifying the most appropriate funding source, tracking and updating actions to fund the requirements, submission of funding requests, and allocation and obligation of funds. A formal DoD AT requirements documentation and prioritization methodology has been established by the Joint Staff and OSD and adopted by the Services and Combatant Commands. The Services, OSD, and Joint Staff use this methodology to document and prioritize AT requirements for both the PPBE and the CbT RIF processes.

(4) (U) For the USNORTHCOM AOR, a comprehensive RM/resource management approach is the linking mechanism for missions, risks, and resources. It provides the essential ground-truth for efficient and effective AT resource management at each organizational level. Ultimately, the linkage of RM with resource management within the AOR will result in higher degree of effective AT mission assurance and operational readiness. Commanders and Directors will use the following guidance to: a) identify and justify AT resource requirements; b) prioritize projects to satisfy the requirements; and, c) ensure risk management is a fundamental consideration throughout the resource process.

(5) (U) Resourcing AT Requirements.

(a) (U) The PPBE process is the primary DoD resource mechanism that results in funding of the DoD Elements. Within the USNORTHCOM AOR, understanding and application of the PPBE process is mandatory, as it serves as the primary funding source to support the AT requirements of the DoD Elements. Given the major influence of Combatant Commands within the DoD PPBE process, the DoD Elements must participate in and support the integrated PPBE process activities of their HHQs and USNORTHCOM.

(b) (U) An important additional funding source is the CbT RIF program. The CbT RIF program helps fund emergency and emergent high-priority CbT requirements in the year of execution. Within the USNORTHCOM AOR, the DoD Elements will use the CVAMP program for development and submission of CbT RIF requests. AOR-wide use of CVAMP will result in enhanced standardization, better understanding and analysis of theater -wide AT issues and problems, and ensure efficient and effective use of all available AT resources. CVAMP is found via SIPRNET on the ATEP portal (http://www.atep.smil.mil/). All users will log into ATEP and set up their profile that will be used to track the submission process. Instructions for CVAMP are located on the ATEP portal. Further information on CbT RIF and how to submit a request can be found in *refs. o and j*. These documents can be found on the NORAD-USNORTHCOM portals:

NIPRNet: https://www.noradnorthcom.mil/j3/j3
SIPRNet: https://www.noradnorthcom.smil.mil/j3/j34

b. (U) Tasks.

(1) (U) USNORTHCOM. The following are USNORTHCOM tasks to essential for theater-wide AT resource optimization and coordination.

(a) (U) Coordinate an annual AT AOR Resource Conference for the DoD Elements. The primary purpose of the conference will be to review and prioritize AT resource requirements from a theater perspective, and, secondly, to review Unfunded Requirements (UFR) and CbT RIF resource trends and priorities affecting the USNORTHCOM AOR.

(b) (U) Develop and implement a theater-wide process for prioritization and submission of CbT RIF requests. In addition, establish a USNORTHCOM CbT RIF Evaluation Panel to standardize and manage CbT RIF submissions.

(c) (U) In coordination with the Joint Staff, standardize constructs and definitions supporting AT resource management and the FP mission.

(d) (U) Develop and disseminate an annual CbT RIF After-Action Summary for the USNORTHCOM AOR. Include lessons learned, trends and issues affecting critical capabilities and AT execution.

(2) (U) DoD Elements: The following are essential AT resource-related tasks for execution by the DoD Elements in the USNORTHCOM AOR:

(a) (U) Participate in and actively support the PPBE process for AT resource requirements definition and optimization in the USNORTHCOM AOR.

(b) (U) Develop and apply an integrated RM methodology within organizational AT resource processes. Ensure that RM addresses operational mission impact within the AT resource requirement definition, development, prioritization and submission process.

(c) (U) Develop and submit CbT RIF and UFR requests within appropriate command/organizational channels. For UFRs forwarded to USNORTHCOM, they can be submitted throughout the year on an as needed basis. CbT RIF request submission deadlines are 1 January and 1 September. However, as individual requests are identified, they can also be forwarded to USNORTHCOM throughout the year.

(d) (U) Annually, by 15 February, provide USNORTHCOM with a Fiscal Year (FY) FP budget summary for the previous and current FYs.

(e) (U) Annually, by 15 April, provide USNORTHCOM with a strategic list of mission-required capabilities that are essential for accomplishment of individual DoD Element FP responsibilities. The list should include description of any major, mission-degrading shortfalls. From the theater perspective, USNORTHCOM will analyze the

DoD Element required capabilities lists, and revise or generate AOR resource-related priorities accordingly (e.g., IPL, adjust FP resource priority recommendations, etc).

(3) (U) Documenting AT Requirements.

(a) (U) CVAMP is the primary means used by USNORTHCOM and the DoD Elements to forward DoD Element-specific AT requirements in support of Commander, USNORTHCOM's resourcing priorities. The DoD Elements in the USNORTHCOM AOR will submit their unfunded AT requirements into CVAMP throughout the year to allow oversight of critical issues as they arise and to help plan accordingly. Suspenses for submissions in support of key USNORTHCOM engagement points are as follows. Submission content requirements for the IPL and POM are detailed in Tab A to Appendix 7.

Integrated Priority List (IPL)	1 August ["on year" only]
Chairman's Program Assessment (CPA)	o/a 15 Sep [each year; review for comment only]
Strategic Planning Guidance (SPG)	o/a 15 Sep [each year; review for comment only]
Program Objective Memorandum (POM)	1 October ["on year" only]
Chairman's Program Recommendation (CPR)	o/a 1 Feb [each year; review for comment only]
Joint Programming Guidance (JPG)	o/a 1 Mar [each year; review for comment only]

(b) (U) AT requirements must be sent simultaneously to the respective HHQs with info copy to USNORTHCOM, ATTN: NC/J34, who will collaborate with and forward them to the N-NC/J8. This will ensure that all decision makers are using the same data.

(c) (U) Services are to ensure that any tenants residing on Service installations coordinate their AT resource requirements with the host installation Commander.

(4) (U) IAW DoDD 2000.12, USNORTHCOM will identify, document, validate, prioritize, and submit to the Joint Staff for advocacy the resource requirements necessary to achieve the AT Program objectives for each activity under the Combatant Commander or for which that Commander has AT responsibility. USNORTHCOM will work with the Joint Staff and the DoD Elements to ensure that resource requirements to implement the AT Programs are identified and programmed according to the PPBE process.

(5) (U) Once requirements are submitted to USNORTHCOM, NC/J34 will conduct a theater risk assessment. This risk assessment facilitates development of a prioritized list for N-NC/J8 to update the USNORTHCOM Commander's Integrated Priority List (IPL).

(6) (U) To assist in the prioritization of resources, requirements will be placed into the following three categories of importance: Must Fund (M), Need To Fund (N), and Should Fund (S). The DoD Elements must maintain awareness of the requirements, their significance, and associated risks. It is not necessary for each criterion within a specific category to be met for that requirement to be identified as Must (M), Need (N), or Should (S). However, a majority of the criteria in Figure C-7-2 should be met.

Criterion and Summary Descriptions for Prioritization Categories

Criterion	Must Fund	Need to Fund	Should Fund
Typical % of Requirements	~10-20%	~30-40%	~50-60%
Threat	High-Significant	High to Moderate	All Threat Levels
Asset Criticality	Likely Target – Critical to Mission – High Impact – Significant Time to Restore to Operations	Likely Target – Moderately Critical to Mission – Large # of People – Moderate Time to Restore to	Asset Important to Mission – Wide # of People – Short Time to Restore to Operations – Redundant Capability exists
Asset Vulnerability	Significant/ Major Vulnerabilities – MILCON Standards not met – Weak Structural Protection– Extremely Accessible and Vital Recognizable Structures	Moderate Vulnerability- Accessible, Lacking Perimeter/ Access Control – Construction Protection Low – Recognizable Important and Lucrative Structures	Lower Vulnerability – Less Accessible, Enhance Perimeter/Access Control – Construction Protection Moderate – Less recognizable structures identified as vulnerable
Current AT Plan/Program Effectiveness	AT Program Ineffective/ Unexecutable - Resources Not Available for Baseline AT Program or higher FPCON measures - No Other Mitigation Capability	AT Program Ineffective/ Unexecutable - Resource may be necessary to execute higher FPCON AT measures - Short-term mitigation capability available	Enhance/Improve AT Program – Resources available for FPCON baseline and baseline +1; however, may be necessary to execute higher FPCON AT measures - Longer-term mitigation capability available

Commander's Risk	Major / High Risk – Unacceptable Impact on Mission Readiness	Considerable/Moderate Risk – Long-term Impact on Mission	Lower Risk – Short-term Impact on Mission Readiness

Figure C-7-2

(7) (U) Selection of requirements identified as an M, N or S signifies that the item/project is affordable, supportable, will reduce risk, and provide a high/moderate impact on the program to achieve the objectives identified in the AT Plan. Once the requirements have been prioritized and categorized, an acquisition strategy needs to be researched, requirements submitted, and funding sources sought. The same requirement should be sent to both USNORTHCOM and the DoD Elements.

(8) (U) Data calls to all DoD Elements will occur as part of the USNORTHCOM PPBE process. The DoD Elements are responsible for identifying their priorities and generating submissions. NC/J34 is responsible for consolidating, vetting and prioritizing inputs and forwarding them to N-NC/J8. N-NC/J8, in collaboration with NC/J34, is responsible for considering them for inclusion in the appropriate resourcing venues. Submissions for the IPL and POM will be IAW the template at Tab A. USNORTHCOM will forward a comprehensive command position to the DoD Elements for each respective PPBE sub-process.

(9) (U) CbT RIF.

(a) (U) USNORTHCOM will accept CbT RIF requests from only one DoD Element POC in the USNORTHCOM AOR, as listed below. The authorized DoD Element is responsible for prioritization within their organization. All submissions for CbT RIF will be entered through the CVAMP on the ATEP: http://www.atep.smil.mil/.

(b) (U) Based upon dialogue/interface with the DoD Elements, USNORTHCOM will accept CbT-RIF from the following the Service sources*.

Dept of the Air Force (Includes the Air National Guard)
Dept of the Army (Includes the Army National Guard)
FLTFORCOM
MARFORNORTH
**Includes Reserves*

(c) (U) The Air Force and the Army have asked NC/J34 to accept CbT RIF submissions directly from their Service. The Air Force and Army will consolidate and submit all requirements for NORTHAF and ARNORTH. Service organizations allocated to Combatant Commands can submit for CbT RIF through that Combatant Command, but cannot dual submit the same request through USNORTHCOM. If the request is for an identified installation vulnerability then that request will go through the Service for submission to USNORTHCOM.

(d) (U) USNORTHCOM will accept CbT RIF submissions from each of its subordinate HQs:

Joint Task Force Civil Support (JTF-CS)
Joint Task Force NORTH (JTF-NORTH)
Joint Task Force Alaska (JTF-AK)
Joint Force Headquarters National Capitol Region (JFHQ-NCR)

(e) (U) Defense Agencies and DoD Field Activities within the USNORTHCOM AOR but outside the NCR are identified below and will make prioritized CbT RIF submissions to NC/J34.

Defense Logistics Agency (DLA)
Defense Threat Reduction Agency (DTRA)
Defense Security Service (DSS)
Defense Commissary Agency (DeCA)
Defense Contract Management Agency (DCMA)
Defense Intelligence Agency (DIA)
National Geo-Spatial Intelligence Agency (NGA)
TRICARE Management Activity (TMA)
Defense Contract Audit Agency (DCAA)
Defense Human Resources Activity (DHRA)
Defense Finance and Accounting Service (DFAS)
DoD Counterintelligence Field Activity (CIFA).
Defense Information Systems Agency (DISA)
DoD Education Activity (DoDEA)
National Security Agency (NSA)
Army & Air Force Exchange Services (AAFES)
Missile Defense Agency (MDA).
Pentagon Force Protection Agency (PFPA)

(f) (U) Defense Agencies and DoD Field Activities within the USNORTHCOM AOR and inside the NCR (identified below) will go through PFPA for all CbT RIF submissions.

American Forces Information Service (AFIS)
DoD Test Resource Management Center (DTRMC)
Defense Advanced Research Projects Agency (DARPA)
Defense Legal Services Agency (DLSA)
Defense Security Cooperation Agency (DSCA)
Defense Prisoner of War/Missing Personnel Office (DPMO)
Washington Headquarters Service (WHS)
Defense Technology Security Administration (DTSA)

(g) (U) Combatant Commands: If the request is for operational issues, the Combatant Command may submit directly to the Joint Staff. If a Combatant Command

resides on an installation in a tenant relationship and the request is for that installation, then the Combatant Command should submit the request through that Service as a tenant on that installation. Combatant Commands are not allowed to dual submit requests through the Service and directly to the Joint Staff for the same request.

USPACOM
USSOUTHCOM
USSOCOM
USSTRATCOM
USTRANSCOM
USJFCOM
USCENTCOM

(h) (U) National Guard Units: CbT RIF is intended for Title 10 forces and National Guard forces providing support to Title 10 missions. Per Joint Staff guidance, all National Guard units that fall under this guidance may submit their requests through the respective Service for consideration/consolidation.

(i) (U) It is important that all submissions go through the appropriate chain of command for accountability and consolidation to ensure duplicate submissions are not received.

(10) (U) Prioritizing CbT RIF Submissions.

(a) (U) NC/J34 will:

1. (U) Conduct initial informal draft review of submitted CbT RIF packet via CVAMP and provide feedback recommendations/comments to the originator with recommendations/comments. Requirements should focus on preventing mass casualties using an outside-to-inside approach emphasizing deterrence, detection, and defending against terrorist attacks. The purpose is to prevent terrorists from accessing DoD installations or facilities inhabited by DoD personnel or their families.

2. (U) Review final CbT RIF submission and staff through USNORTHCOM. At a minimum, NC/J34 will staff CbT RIF packets through N-NC/J8, N-NC/JA, N-NC/J4, NC/J3, and Commander, USNORTHCOM or Deputy Commander, USNORTHCOM before submission to Joint Staff DD AT/HD via CVAMP. Every effort will be made to forward the DoD Elements' concerns and priorities while ranking CbT RIF submissions. USNORTHCOM will validate and prioritize CbT RIF submissions by conducting a review board consisting of the NC/J34 branches and N-NC/J4 engineering and following the guidance set forth by *ref. a*. The board will conduct vetting and prioritization of the requests 2 weeks before the Joint Staff suspense for CbT RIF submissions. Requests will be prioritized by the CVAMP numerical score and utilizing the outside to inside approach. The outside to inside analysis will help in further prioritization by elevating submissions which support interdiction far from the installation.

3. (U) Forward USNORTHCOM-approved CbT RIF packages to the CJCS (JS DD AT/HD) for review and funding. If multiple CbT RIF packages are submitted, NC/J34 will provide a USNORTHCOM ranking in the forwarding endorsement to CJCS (JS DD AT/HD).

4. (U) Provide certified funds using a Military Interdepartmental Purchase Request (MIPR) to the assigned forces, Service, Installation, Unit, or Defense Agency/DoD Field Activity comptroller upon CJCS approval of CbT RIF packet and transfer of funds to USNORTHCOM. All CbT RIF funds must be obligated and on contract within 90 days after funds are released from the Joint Staff (except during the final FY quarter which may be less than 90 days).

5. (U) Receive copies of MIPR acceptance from the respective installation as soon as the MIPR arrives at the installation that is executing the project. Receive copies of all contracts as soon as they are awarded for the given project and receive obligation reports from each installation executing a project by the 1st of each month.

6. (U) Provide obligation and expenditure status of all approved requests to the CJCS (JS DD AT/HD) IAW *ref. a* (4.c).

7. (U) Work with the DoD Elements and N/NC-J8 to ensure excess monies are returned to the JS via Programming and Budget Automated System (PBAS).

Tabs:

Tab A. IPL and POM Submission Template (U)

APPENDIX 8 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
LOGISTICS SUPPORT FOR AT (U)

(U) References: *Base Order*.

a. (U) TM 5-853/AFMAN 32-1071.

b. (U) Mil Handbook 1013/1A.

c. (U) DoD Directive 4270.5.

d. (U) ED 61-4.

1. (U) Situation. *Base Order*.

2. (U) Mission. Base Order.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) This critical task is derived from DoDI 2000.16 standards 5, 16, 26, 28 and 29 as well as DoDD 2000.12 requirements 5.14.1, 5.14.7, 5.14.8, 5.15.1, 5.15.7, 5.15.8, 5.17.1, 5.17.2, 5.17.4, 5.17.5, 5.17.6 through 5.17.13, and 5.17.16 through 5.17.18. Although the DoD Elements are responsible for contracting and construction programs under Title 10, compliance with AT guidelines and instruction is critical to prevent and/or mitigate against potential terrorist attacks. Processes must be developed for USNORTHCOM to validate that AT requirements are being met under established Service, Defense Agency and DoD Field Activity construction and contracting programs.

(2) (U) Construction Standards. Terrorist attacks may occur at any time, at any location, and take many forms. While terrorists have many tactics available to them, they frequently use explosive devices when targeting large numbers of DoD personnel with the intent of producing mass casualties. Most existing DoD buildings offer little protection against such terrorist attacks or the threat of chemical, biological or radiological attacks. By applying the guidance in this Appendix the opportunity for such attacks and their effects may be reduced. Application of the AT construction standards alone will not prevent injury or loss of life from a determined terrorist group, but will reduce risk considerably and should be factored into aspects of AT planning.

(3) (U) Contractor Considerations. The incorporation of AT considerations into commercial relationships with foreign and local merchants and service providers is essential to enhancing the AT posture of supported forces. If given a vested interest in the safe passage of U.S. forces, local merchants and service providers can put local

culture, knowledge and expertise to work in protecting U.S. forces, especially for in-transit forces. Therefore, during the process to establish logistics requirements and during the contracting award, execution and evaluation process, AT measures and actions should be considered, particularly when the contracted support could affect the security of operating forces. Additionally, the awarding of future contracts should be contingent upon the performance of adequate AT measures.

b. (U) Tasks.

(1) (U) AT Construction.

(a) (U) This Appendix supplements the UFC (*ref. m*) and describes additional minimum AT construction design standards that must be incorporated into all DoD-inhabited structures in the USNORTHCOM AOR. Where differences between this appendix and the UFC exist, the more stringent standard will be applied.

1. (U) For new construction and major renovation, the identified standards will be incorporated into the PPBE process for construction activities.

2. (U) Commanders will initiate programs to assess existing structures in accordance with current standards and determine vulnerabilities. While no formal timeline is mandated for the completion of upgrades, DoD Elements should prioritize assessment results according to specific risks at each site. The intent of the existing facility assessments is to provide data to Commanders, which supports future upgrades. Commanders should use this data and local security risk assessments to identify and prioritize needed improvements as part of routine facilities upgrades and support requests for additional funding.

3. (U) For existing leased inhabited facilities that do not meet the minimum design standards, it is recommended these leases not be renewed. If a new lease contract is entered into, the following standards must be incorporated as outlined below.

4. (U) Service Headquarters, Combatant Commands, Defense Agencies and DoD Field Activities operating in the USNORTHCOM AOR will incorporate DoD and USNORTHCOM supplemental design standards to minimize the risk to personnel from terrorist attack.

5. (U) Minimum design standards are set by the JS through the UFC. USNORTHCOM sets forth additional recommendations. Services, Defense Agencies and DoD Field Activities are responsible for ensuring these standards are implemented and that subordinate installation Commanders certify that FP considerations have been incorporated into the project programming/design/construction process (DD Form 1391, design approval, etc.). Installation Commanders must certify that higher levels of protection resulting from more severe threats are not required for each project. A

procedure for determining the appropriate threat severity and level of protection can be found in *refs. a and b*.

6. (U) Although specific minimum standards are provided, inhabited structures will be designed or modified to achieve a low level of protection against the blast loads from mortars, rocket propelled grenades (RPGs), and improvised explosive devices (IED) with explosive equivalents of 100 kilograms of TNT at the required/available standoff distances. This should be done unless it has been determined that a higher threat severity exists and/or a higher level of protection is warranted.

7. (U) At a minimum, one planning/design engineer from each DoD Element will be trained in "Security Engineering". The U.S. Army Corps of Engineers (USACE) Security Engineering course fulfills this requirement. The USACE, Omaha District, Protective Design Center (CENWO-ED-S) is currently the only identified agent for scheduling this training.

(2) (U) Standards.

(a) (U) See *ref. m*.

(b) (U) Additional Design Considerations/Compensatory Measures. Although not specifically required, the measures listed below should be considered for incorporation in the design and construction of inhabited facilities.

1. (U) Perimeter Counter-Mobility. All sites should have a physically secured perimeter that includes a continuous barrier that marks the perimeter boundary and that provides a physical obstacle to vehicle penetration.

a. (U) If threat analysis does not identify a moving vehicle bomb tactic, these barriers need not provide physical resistance to stop vehicles, only make it difficult to cross the boundary without drawing attention. The aggressor's goal in the stationary vehicle bomb tactic is to remain covert until the device is detonated.

b. (U) The barriers on the secured perimeter must be designed to stop the moving vehicle where vehicle approach to the perimeter is possible. Vehicle weight, maximum attainable velocity, and angle of impact will be considered when selecting crash rated perimeter barriers. Calculate requirements by using procedures in *refs a and b*.

(c) (U) Perimeter Security and Control of Entry to Site. Consider protecting the installation by a perimeter security fence through which access is controlled at an established access control point. Effective security lighting at the entry points to support the security check and inspections must be addressed at the design stage. Installations with perimeters adjacent open water will take appropriate steps to prevent unauthorized access and water borne threats from this direction.

1. (U) The access control point must be able to process vehicles in such a way that during increased FPCON entry is not impeded, thus impairing traffic flow. The reason for this is twofold:

a. (U) To prevent personnel awaiting entry from becoming vulnerable to attack; and

b. (U) To prevent pressure being put on the guards to forgo security checks in order to speed up traffic flow.

2. (U) The control of entry system should include provisions for visitor parking, a pass office, search areas, guard positions, and a turning area where unauthorized vehicles may be turned around and ejected from the facility/installation without gaining access.

3. (U) Where indicated by threat analysis, provide shielding or hardening of the guard structure to protect access control point guards against drive-by attacks using small arms. The access control point should employ active vehicle barriers appropriate for the threat and integrated with the passive perimeter barriers to ensure there are no weak spots in the perimeter. However, professional advice should be sought before installing some active barriers such as pop-up barriers in order to ensure that the proposed equipment is operationally effective.

(d) (U) Access Roads. Consider main headquarters building and area sites where large numbers of personnel congregate, away from local roads outside the perimeter and away from primary access roads onto the facility. This will reduce vulnerability to vehicle-borne explosive devices and standoff attack.

(e) (U) Protected Areas. Consider the incorporation of Protected Areas (PA). A PA is a specifically designated area within a building where vulnerabilities from blast effects of an explosion are minimized. It is a location where occupants are advised to go in the event of a bomb threat warning. Consider this at the design stage for new construction. In existing buildings, professionally qualified structural engineers with experience of explosive effects should undertake PA identification. A PA should meet the following minimum criteria:

1. (U) Away from windows, external doors and external walls.

2. (U) Toward the center of the building.

3. (U) Generally not in stairwells or areas having access to an elevator shaft since blast overpressures are likely to propagate into these areas.

4. (U) Locate in areas surrounded by full height masonry or concrete walls if possible, e.g., internal corridors, internal toilet areas, etc.

5. (U) The size of the room(s) must be such that it will provide a minimum of 0.9 square meters (10 square feet) of space for each person who will occupy the room.

(f) (U) Location of HRP Offices. Consider locating HRP offices away from over-looking points. These offices should not be sited in areas that would make the HRP vulnerable to standoff attack. Office layout should also bear this in mind. Consider the use of bullet resistant glass. Where possible, cover or protect the arrival/departure area for HRPs to increase their safety at this vulnerable stage of movement.

(g) (U) Search/Screening Areas. Consider the incorporation of separate search/screening areas at entry points to facilities that would be attractive targets of terrorists (e.g., headquarters buildings). Search/Screening areas should provide a place where personnel desiring entry, who are not preauthorized, could be taken and searched if necessary. A search/screening area also provides an area where a person can wait until his/her credentials are confirmed. A separate area for this function relieves the pressure on the security guard force performing routine pass and identification checks.

(h) (U) Personnel Alerting Systems (PAS). Consider the incorporation of building and installation PAS so that personnel can be warned via audible alarm and given directions as to what to do in the event of an attack or emergency by voice messaging. PAS systems should be capable of warning and directing personnel for various emergencies such as bomb attack, mortar attack, fire, and earthquake.

(3) (U) N-NC/J4 will plan for and participate in CIP related programs, as well as assist NC/J34 to coordinate and make recommendations on unresolved AT facility requirements during programming and budget reviews. N-NC/J4 will establish procedures with the DoD Elements to verify that all AT design construction standards meet the UFC. Services are responsible for documenting their facility requirements through respective chains of command, using the UFC.

(4) (U) Deviation Program. N-NC/J4 is coordinating with NC/J34, OSD and the Senior Engineer Working Group (SEWG) to develop specific AT construction deviation request procedures for the USNORTHCOM AOR. In the interim, the DoD Elements will, IAW ref. m, paragraph 1-1.2.3, continue to utilize Service and Agency-specific AT construction and deviation request processes. DoD Elements will submit AT construction deviation requests through their respective Service chains of command to OSD and will provide copies of Service approved deviation requests to USNORTHCOM for the following structures: billeting, primary gathering buildings, and *Critical Facilities (ref UFC 4-010-01, paragraph 1-5.3). N-NC/J4 will consolidate these requests into an annual report to Commander, USNORTHCOM NLT 30 September of the current Fiscal Year (FY). Commander, USNORTHCOM retains the right to review and make change recommendations to OSD on these deviation requests. *(*Critical Facilities is defined by*

UFC 4-010-01, paragraph 1-5.3 as: Buildings that must remain mission operational during periods of national crisis and/or if subjected to terrorist attack should be designed to significantly higher levels of protection than those provided by these standards.)

(5) (U) Contractor Considerations.

(a) (U) N-NC/J4 will ensure through the DoD Elements that programs are in place to validate logistics support contracts and agreements to consider AT where applicable. DoD Elements are responsible to ensure the logistics contracting process for support of forces will incorporate considerations for AT measures during the contract award process, and the execution and evaluation process when the effort to be contracted for could affect the security of forces residing, exercising, operating in, or transiting through the USNORTHCOM AOR. DoD Element AT Program offices will identify their logistics POC for this process and coordinate with N-NC/J4 to establish reporting processes to validate these requirements. The contract support process will be incorporated and addressed in the vulnerability assessment process and assessed during HHQs Assessments.

1. (U) Responsibilities: Services, Defense Agencies/DoD Field Activities are responsible for applying AT considerations in the logistics planning process and for ensuring that AT requirements are incorporated where applicable in support contracts to include contracting requirements, award, execution, and evaluation:

a. (U) Incorporate AT considerations into commercial relationships in order to develop a vested interest, on the contractor's part, for ensuring the safety and security of U.S. forces.

b. (U) Include where applicable in support contracts measures for limiting access to in-transit units. This effort should include the establishment of exclusion zones and the badging of contractor personnel and the flagging of support vehicles/boats so legitimate workers can be easily identified.

c. (U) Where applicable, include review of company personnel hiring policies and processes to ensure they adequately screen for applicants that present security risks via the Terrorist Screening Center.

d. (U) Incorporate flexibility into logistics contracts so that routine schedules and predictability can be avoided.

(b) (U) Contract Review. Upon receipt of services or support from logistics contracts, Commanders normally are required to submit customer service reports back to their contracting office. At this time that the Commander should review those applicable AT measures that were and/or were not utilized. From this review, Commanders may select to upgrade contractual agreements as appropriate to ensure AT measures are adequate in the future. Any upgrades will need to be coordinated with the contractor and may require negotiation. Where those existing AT measures were

found inadequate and can be mitigated using contracted security provisions, the Commanders should consider supplementing the contract. In cases where extra contract security measures are not a viable option, Commanders should coordinate with their appropriate AT staff elements to ensure an appropriate level of FP is provided.

(c) (U) Contracts. Contracted AT measures and external security, if needed, strengthen the AT posture of in-transit units and should be implemented through logistics contracts and transportation agreements. Most contracts, especially those supporting USNORTHCOM transiting forces within the AOR, fall into one of the following categories:

1. (U) Sea port Fuel Contracts.

a. (U) The preferred means to provide supply support to Naval Forces en route to CONUS is by underway replenishment (UNREP) from Combat Logistics Force (CLF) ships, which are located in the logistics arm of a Carrier Battle Group (CBG).

b. (U) It is a Navy operational decision if single transiting ships will refuel en route under a Defense Energy Support Center (DESC) contract. There are Defense Fuel Support Points (DFSP) and DFSC Bunkering contracts at commercial ports in the USNORTHCOM AOR.

2. (U) Sea port Husbanding Agent (HA) Contracts.

a. (U) HA contracts provide both supplies and services in port.

b. (U) Supplies provided are typically those refrigerated food items that must be restocked during long transits. This includes fresh fruit, vegetables and dairy products, as well as water.

c. (U) Services contracted are typically diverse in nature.They may include trash removal, sewage removal, waste oil removal, port services handling, feeders and line handlers, berthing and port fees (where allowed), tug and pilot services, forklift and crane services, bus services with driver and telephone services.

d. (U) The Navy administers HA contracts in CONUS.

3. (U) Airport Servicing and Fueling Contracts.

a. (U) Upon arrival in CONUS, tactical units are supported using organic resources. Depending on the location, AMC or commercially contracted carriers are supported by US, or commercially contracted support elements.

(d) (U) Local Contracts. These contracts consist of support for supplies and services, AT measures for such contracts are strictly administered from bed down sites/installations in the AOR.

(e) (U) The Federal Acquisition Regulation (FAR) does not require Contractor vetting/background investigations; however, the FAR requires a determination of contractor responsibility before contract award. According to the FAR, a potential contractor must "have a satisfactory record of integrity and business ethics". This provision may allow exclusion of potential contractors that have ties to terrorists or criminal organizations and also permits a more comprehensive background check of contractors. Other service providers not under contracts governed by the FAR, such as host nation port and airport personnel and some transportation providers, should be vetted where feasible.

(f) (U) Where applicable, contracts must include provisions for AT measures. These provisions must at a minimum cover:

1. (U) Vetting of contractors to include review of hiring processes and policies to ensure personnel who present a security risk are properly identified and screened out.

2. (U) FP responsibility for contractors.

3. (U) That contractors must comply with all USNORTHCOM AT provisions of this instruction.

(g) (U) The checklist provided in Tab B to this appendix can be used for contracting in support of the overall AT Program.

(h) (U) DoD Contractors. By law and under current DoD policy, FP responsibility for U.S. citizens (to include DoD contractors, their employees, and their family members) rests with the contractor. DoD has no legal obligation for AT of DoD contractors or contractor employees unless specific language is included in the contract. Contractor employees who live or work on U.S. installations benefit from some of the same security measures provided to service members by virtue of their location. However, contractor employees who work off base or who reside on the local economy do not receive these indirect benefits, thus must provide for their own security. In accordance with DoDD 2000.12, DoD contractors within the USNORTHCOM AOR will:

1. (U) Provide AT awareness information to their employees (before travel outside of the US) commensurate with the information DoD provides to its military, DoD civilians and families (to the extent such information may be made available).

2. (U) Comply with the requirements set forth in DoDD 4500.54 prior to travel outside the US

c. (U) Coordinating Instructions.

(1) (U) Points of Contact.

(a) (U) The following points of contact and references may prove useful when applying the guidance in this appendix.

1. (U) The Joint Staff DD AT/HD Division is the single POC and coordinator for AT matters on the Joint Staff. Phone: (703) 693-7562 x 105

2. (U) USACE South Atlantic District, Mobile Office is a construction agent for the design and construction execution of facilities in the USNORTHCOM AOR. They coordinate security engineering with the U.S. Army Corps of Engineers' Protective Design Center in Omaha, Nebraska, and other centers of expertise.

3. (U) Atlantic Division, Naval Facilities Engineering Command (LANTDIV). LANTDIV is a construction agent responsible for design and construction execution of facilities in the USNORTHCOM AOR. As such, they coordinate blast engineering with the Naval Facilities Engineering Service Center in Port Hueneme, California.

4. (U) HQ NORTHAF/CEW is a construction agent responsible for design and construction execution of facilities in the USNORTHCOM AOR. They receive support from the Air Force Civil Engineer Support Agency, Tyndall AFB, Florida, the lead Air Force engineering center for force protection.

5. (U) DTRA. DTRA is the lead agency for conducting Joint Staff sponsored blast testing and VAs.

6. (U) Design and execution of minor construction and O&M funded repair work are typically accomplished by the Service Headquarters or DoD Element command having jurisdiction and regional responsibilities for construction/engineering management, as defined in DoD Directive 4270.5, and/or ED 61-4, Appendix B-1.

4. (U) Administration.

a. (U) Reporting Requirements. *Annex R, Reports.*

Tabs:

A. Sample Request for Deviation (U)
B. Checklist for Use in Contracting Support (U)

APPENDIX 9 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
INSTALLATION CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR AND HIGH-YIELD EXPLOSIVES (CBRNE) PREPAREDNESS (U)

(U) References: *Base Order*.

1. (U) Situation. *Base Order*.

a. (U) Purpose. This critical task is derived from the DoDI 2000.16 standards 2, 5, 10, 14, 17, 18, 20, and 23 and DoDD 2000.12 requirements 5.15.9, 5.17.1 through 5.17.5, 5.17.8 through 5.17.13 and 5.17.16 through 5.17.18. The responsibility to integrate CBRNE training, exercises, and plans into overarching AT plans is critical for synchronized operations. USNORTHCOM's responsibility is to establish the process to ensure policy and plans are developed that focus Installation CBRNE Preparedness, to include interface with local civilian communities.

2. (U) Mission. *Base Order*.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) DoD Elements within the USNORTHCOM AOR will implement a comprehensive Installation CBRNE Preparedness program. As it may be impossible to determine if a CBRNE release was an accident or a deliberate incident, the USNORTHCOM Installation CBRNE Preparedness program must include an all-hazards approach.

(2) (U) The primary end state is: Protect Personnel, Maintain Installation Critical Missions, and Restore Essential Installation Functions.

(3) (U) Installation CBRNE Preparedness will be accomplished through a tiered installation approach, utilizing four Principles of Installation CBRNE Preparedness. Minimum standards are delineated within each Principle by Installation Category (See Tab A (Installation Categories)). Installations with appropriate resources may exceed Installation Category minimum standards. Details regarding installation categories and capabilities are shown in the Planning Considerations (Figure C-9-1).

Installation Categories	CAT 1	CAT 2	CAT 3	CAT 4	CAT 5
Capabilities					
Sense 1	Desired				
Sense 2	Required	Required	Desired		
Shape	Required	Required	Required	Required	
Shield 1	Required	Required	Required	Required	Required
Shield 2	Required	Required			
Sustain	Provided by external federal, State, and local Agencies (and host nation as applicable)				

Figure C-9-1

(4) (U) Installations who cannot meet required capabilities will coordinate for those capabilities with local, State, Federal authorities or adjacent installations.

(5) (U) CBRNE Planning Considerations.

(a) (U) Threat. Terrorist may try to destroy, disrupt or exploit key U.S. military capabilities. Threats include:

1. (U) Chemical. Terrorists may exploit a myriad of toxic industrial chemicals (TICs) available in all parts of the globe. These substances are not likely to create as many actual casualties as warfare-strength agents, but are still lethal or highly toxic. Chemical agents can be dispersed using mortars, sprayers, and improvised explosive devices. Chemicals can last from minutes to weeks at the site of release and create a larger initial hazard area than conventional explosives. Further, chemicals often create a temporary downwind vapor hazard.

2. (U) Biological. Biological hazards pose unique challenges because they are relatively easy to produce and difficult to detect after release. Examples of terrorist biological weapons include small amounts of anthrax or smallpox dispersed using a non-explosive point source or spray tank. The duration of agent virulence and the size of the downwind hazard area are largely dependent on environmental conditions and dissemination efficiency at the time of the attack. The potential psychological impact and relative low cost of biological hazards make them an attractive alternative to explosives. Offensive biological programs can be easily concealed, and production does not always require specialized equipment. Effective medical intervention is possible for many bacteria, but other pathogens (e.g., viruses, fungi, toxins) can be much more difficult to treat.

3. (U) Radiological. Low-level radiological material is available from a large number of industrial sources worldwide. Terrorists able to gain access to this material could exploit it using low-yield explosive devices. Specific examples of terrorist radiological hazards include iridium, cesium, and highly enriched uranium (HEU) as the core of a radiological dispersal device. Although rarely lethal in the near term, the

deliberate dissemination of radioactive matter can cause considerable immediate psychological harm and enormous remediation/restoration

4. (U) Nuclear. Terrorists with sufficient finances will seek out those willing to sell both information and materiel regarding nuclear weapons. Besides the extremely high explosive nature of nuclear weapons, other effects include high-altitude electromagnetic pulse (HEMP/EMP) that can degrade unprotected and vulnerable military and civilian electronics.

5. (U) Explosive. Virtually every country, sub-national group, and terrorist organization has access to explosive devices. Traditionally, these have been the weapons of choice to terrorists because they are readily available, cheap, easy to use, and their effects are reasonably predictable. Although there is considerable psychological impact with terrorist use of an explosive devise, most actual casualties are created in the immediate area of the blast.

(6) (U) USNORTHCOM will utilize the Sense, Shape, Shield, and Sustain (4S) construct (as outlined in ref. ff) for CBRNE PREPAREDNESS. However, the AT community uses slightly different terms to discuss their preparedness capabilities. The AT community uses DETECT and ASSESS (as opposed to SENSE); REPORT (as opposed to SHAPE); PREVENT/DETER and DEFEND (as opposed to SHIELD); and RECOVER (as opposed to SUSTAIN). Provided below is an overlay depicting how the four PRINCIPLES FOR INSTALLATION CBRNE PREPAREDNESS and the AT PRINCIPLES parallel each other:

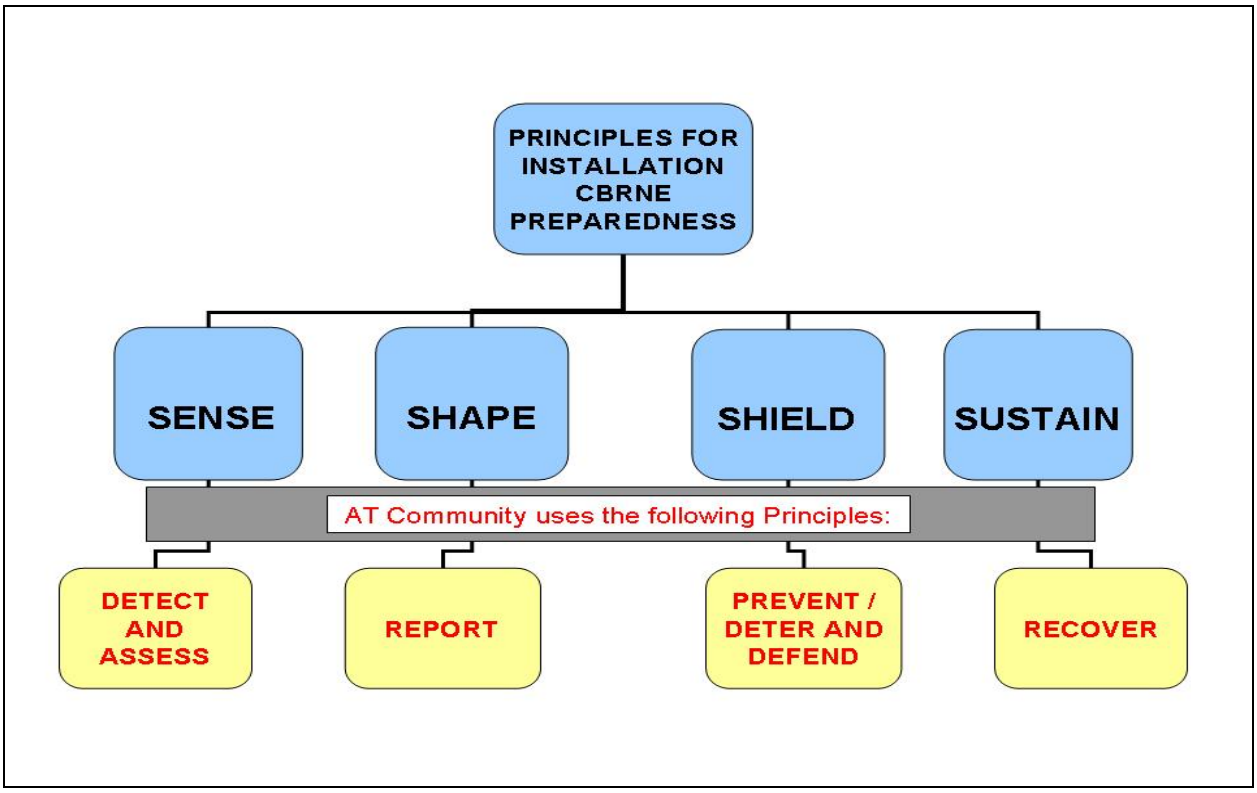


Figure C-9-2

(a) (U) SENSE: The ability to maintain awareness of the current CBRNE situation by detecting and identifying CBRNE hazards in the air, water, food, or soil, on personnel, equipment or facilities, and determining the physical state of those hazards (solid, liquid, gaseous). This principle includes the capability to quantify and sample CBRNE hazards. Sense is the key enabler, using knowledge-based human and state-of-the-art detection equipment, for shaping the installation Commander's understanding of the hazard. SENSE categories are as follows:

1. (U) Sense 1, Stand-off Detection and Reconnaissance.

a. (U) Stand-off detectors can increase the effectiveness of early warning of CBRNE hazards and assess large areas for potential contamination, thus allowing the commander to make rapid decisions on active defense, evacuation, shelter-in-place, and other protective measures. The employment of these sensors calls for careful placement to provide adequate coverage, and often can require specialists to operate.

b. (U) Reconnaissance. If an installation or facility lacks the ability to perform stand-off or automated point detection, it may fall to dedicated CBRNE specialists or installation emergency responders to reconnoiter the hazard area with specialized equipment as the incident unfolds.

2. (U) Sense 2, Automatic Point Detection and Medical Surveillance.

a. (U) Automatic and manual point detectors offer installation personnel tools to detect, identify, quantify, and sample CBRNE hazards to provide decision makers with critical information. Since point detectors by their nature only inform personnel in the immediate vicinity of potential hazards, it is crucial that these detectors be emplaced at critical sites on the installation and networked into the emergency operations center. If the use of automatic detectors at critical sites is not a feasible option, the installation Commander may need to utilize emergency responders with appropriate manual detectors and communications equipment. The intent is not to employ 24/7 monitoring capability but rather to allow automatic detection and identification capability in times of increased threat conditions.

b. (U) Medical surveillance. Although medical surveillance is a broad area supporting force health protection in general, the reporting of non-battle disease injuries is a critical function. Combined with local (civilian) health surveillance and worker absentee data, the medical specialists should note and report trends in health that may be indicative of a BW terrorist attack.

(b) (U) SHAPE: The ability to provide the capability to characterize the CBRNE hazard for the installation Commander. CBRNE hazard characterization is the process by which the installation Commander develops a clear understanding of the current and predicted CBRNE hazard situation, envisions critical mission end states, and develops the sequence of events that moves the installation from its current state to those end states. By manually and automatically collecting and assimilating CBRNE hazard information from civilians, military personnel, host nation (as applicable), and local/State/Federal response assets in near real time, the commander is able to observe actual and potential effects of CBRNE hazards and to make timely decisions. SHAPING categories consist of:

1. (U) Decision Support Tools. Utilize existing/future command and control systems and resources to ensure accurate assessment and dissemination of CBRNE hazards to the installation population and with military, local, State and Federal emergency operations centers. Installation command centers require CBRNE Preparedness decision support tools that access and assimilate CBRNE hazard data from throughout the installation. Hazard prediction tools must reside with command and control equipment that is ideally interfaced with automated sensors on an installation. In addition, these tools must include the ability to input meteorological, medical, and terrain data that influences the CBRNE hazard effects on a near-real time basis as well as for predictive analysis, allowing the installation Commander to determine the risk associated with various courses of action.

2. (U) Mass Alert Notification. Installations must have the capability to notify, within 10 minutes, all personnel on an installation, as well as affected military personnel and dependents off-site of an impending or actual CBRNE hazard incident. Signals and notifications must be clear and unambiguous to avoid confusion.

Additionally, installations must ensure that their warning system can pass alerts to local regional response systems in order to alert surrounding communities to hazards.

(c) (U) SHIELD: The installation Commander shields his/her personnel when by providing appropriate levels of physical protection, training and medical pre-treatment, to the extent possible. The installation Commander relies on First Responders as the second tier of shielding installation personnel. This is accomplished through the rapid response, assessment, and initial recovery operations undertaken to safeguard personnel from continued hazards, to control contamination, and to initiate steps to restore the area to its pre-incident conditions.

1. (U) Shield 1. Mission essential personnel protection will provide the appropriate level of protection necessary to support mission continuity for up to 12 hours. Non-mission essential personnel protection will provide protection or procedures necessary to survive and incident safely. Evacuation and/or shelter in place procedures are preferred over issuing protective mask and suits. The goal is to have 90 percent of the installation/facility (DoD-leased, -owned, or -managed) initiating evacuation or shelter-in-place measures within 15 minutes of incident notification. Minimum first responder capabilities (for those organizations that have organic first responder capabilities) are outlined in Tab B. Those installations/facilities that have limited or no first responder capability must insure that they are integrated into the host installation or local community first responder notification and response plans.

2. (U) Shield 2. Installation emergency responders are responsible for assessing the hazard and saving lives. Installation emergency response equipment must meet National Institute for Occupational Safety and Health (NIOSH), National Fire Protection Association (NFPA), and all other applicable standards that address operations in CBRNE hazard environments. Emergency medical technicians and hospitals will require medical diagnosis tools and medical countermeasures for CBRNE hazards. Installation Commanders should consider off-installation response capabilities as well as on-installation.

(d) (U) SUSTAIN: SUSTAIN consists of dedicated military units and civilian response agencies organized, equipped, and trained to decontaminate and treat personnel, equipment, and critical infrastructure facilities to regain their full capability as quickly as possible. In most situations, installation Commanders will not be able to maintain and sustain an inherent capability to continue long-term recovery and restoration efforts and return the installation to pre-incident conditions. Installations should identify and determine the capabilities of their applicable civilian response agencies that may be available should a CBRNE incident occur. The successful completion of this task will require prior planning and agreements with local, State, and Federal emergency response agencies.

b. (U) Tasks.

(1) (U) USNORTHCOM will**:**

(a) (U) Exercise overall responsibility to protect, prevent loss or mitigate loss of personnel, critical missions, and assets on DoD installations or facilities within the USNORTHCOM AOR under the authority of TACON (for FP).

(b) (U) Coordinate with the DoD Elements to categorize all installations and facilities IAW Tab A (Installation Categories) in order to determine the appropriate CBRNE preparedness level.

(c) (U) Ensure information/intelligence requirements address CBRNE specific issues.

(d) (U) Develop a process that rapidly identifies if a CBRNE threat is directed towards an installation or facility.

(e) (U) Coordinate and partner with DoD and non-DoD agencies regarding CBRNE preparedness.

(f) (U) Ensure CBRNE is addressed in all plans, orders and exercises. Review and provide input to higher headquarters CBRNE policy.

(g) (U) Establish CBRNE assessment standards/benchmarks. Incorporate CBRNE standards in NC program reviews and vulnerability assessment program IAW Annex C.

(h) (U) Identify, document, validate, prioritize and submit to the Joint Staff resource requirements necessary to ensure the installation CBRNE preparedness. This process is addressed in Appendix 7, paragraphs b.(3) thru (10), pages C-7-4 thru C-7-9.

(i) (U) Develop CBRNE remediation and risk mitigation measures for the protection of installations and maintain a database of those measures.

(j) (U) Ensure CBRNE warning and reporting requirements are addressed in information architecture requirements and development.

(k) (U) Perform HHQ vulnerability assessments triennially IAW CBRNE/Contingency Operations VA, format TBD. Report results of VA on CVAMP or similar IT architecture within 30 days.

(l) (U) Develop appropriate plan to respond to CBRNE events on DoD installations within the USNORTHCOM AOR.

(2) (U) DoD Elements will:

(a) (U) DoD Elements within the USNORTHCOM AOR will implement a comprehensive Installation CBRNE Preparedness program as outlined in paragraph 3 of this Appendix. Training and Exercise requirements are outlined in Tab C (Installation CBRNE Preparedness Training and Exercises).

(b) (U) Pass information and intelligence regarding CBRNE through existing information/intelligence reporting channels/requirements outlined in Annex C Appendix 1.

(c) (U) Coordinate and partner with Federal, State and local authorities regarding installation CBRNE preparedness.

(d) (U) Address CBRNE in all operational plans, orders and exercises to ensure installation CBRNE preparedness capabilities are maintained.

(e) (U) Categorize their installations and facilities in order to determine the appropriate CBRNE preparedness level. Provide USNORTHCOM an annual list of their installations by category IAW Tab A.

(f) (U) Develop AT Physical Security Plans that integrate facilities, equipment, personnel and procedures to maximize CBRNE preparedness.

(g) (U) Provide for remediation and mitigation of CBRNE vulnerabilities for installations and facilities.

(h) (U) Conduct an annual vulnerability assessment on all installations and facilities. All assessments will be provided to the USNORTHCOM J34 Assessments Branch and loaded in CVAMP. USNORTHCOM will establish CBRNE assessment standards at a date TBD.

(i) (U) Identify, document, validate, prioritize and submit to USNORTHCOM resource requirements necessary to ensure the installation CBRNE preparedness. PPBE submissions and CbT RIF are outlined in Annex C, Appendix 7.

(j) (U) Report initiation of any CBRNE incident response plan through the proper chain of command IAW *Appendix 1, paragraph b.(1)(h) Crisis Reporting*. Notification will include the NCOC.

(k) (U) Consider the establishment of a CBRNE Preparedness Officer at the installation level to work in conjunction with the AT Officer/staff.

(l) (U) Establish clear command, control, and communication lines between local, State, Federal, and Host Nation emergency assistance agencies that detail support relationships and responsibilities.

(m)(U) Address Top 3 CBRNE issues in DoD Element monthly FP update. *Annex R, Reports*.

(n) (U) Provide USNORTHCOM with:

1. (U) Tasking POCs for their CBRNE program offices.

2. (U) 24-hour operations center contact information, or 24-hour POC if no operations center is available.

3. (U) Information necessary for NC/J34 to establish accounts/passwords for access to the website/restricted portal.

4. (U) Ensure all information is current and updated on a monthly basis.

(o) (U) Ensure that the Medical Response and IM Program are integrated into the Command's FP Program.

Tabs:
A Installation Categories (U)
B First Responder Minimum Requirements (U)
C Installation CBRNE Preparedness Training and Exercises (U)

TAB A TO APPENDIX 9 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
INSTALLATION CATEGORIES (U)

1. (U) General Information. USNORTHCOM Installation Categories. DoD-owned, -operated, -leased (delegated and non-delegated), or -managed facilities will have the appropriate level of protection. Those installations identified as critical to the execution of the National Military Strategy and the USNORTHCOM Mission require capabilities that deter attacks, maintain mission continuity through CBRNE incident/attack, efficiently regain full operational capabilities after an attack, and capabilities to protect all other non-mission essential personnel. All other installations will require capabilities to protect personnel during an attack, mitigate and effectively react to CBRNE incident/attack. In order to standardize CBRNE Preparedness capabilities, installations are categorized as follows:

a. (U) CAT 1 – Large/Critical Installations. Installations or facilities with more than 15,000 personnel (including military personnel, government civilians, dependents, contractors, and other personnel who work and/or live on an installation or facility on a daily basis); those installations and facilities designated by a Service or Combatant Command because of criticality of mission; or those designated as critical through the DoD CIP.

b. (U) CAT 2 – Emergency Response Installations. Those installations or facilities with an inherent emergency response capability and populations between 2,000 and 15,000 personnel. Category 2 will not contain installations or facilities designated as critical by the Services or Combatant Commands or designated by the DoD CIP.

c. (U) CAT 3 – Non-Emergency Response Installations. Those installations or facilities like Category 2 installations except that they do not have an inherent emergency response capability (requires emergency responder support from external Federal, State, or local emergency agencies). Category 3 will not contain installations or facilities designated as critical by the Services or Combatant Commands or designated by the DoD CIP.

d. (U) CAT 4 – Smaller Installations/Facilities. Those installations or facilities without an inherent emergency responder capability (requires emergency responder support from external Federal, State, or local emergency agencies) and with at least 300 but less than 2,000 personnel. Category 4 will not contain installations or facilities designated as critical by the Services or Combatant Commands or designated by the DoD CIP.

e. (U) CAT 5 – Facilities with less than 300 personnel. Those DoD-owned or -leased facilities, vessels, and operations providing support to U.S. military operations. This includes all DoD-owned or -leased vessels used to facilitate movement of geographical combatant command TPFDD and/or throughput. It also includes those operations at leased seaports of debarkation (SPOD) areas (including all vessel and stevedore support) and airlift operations at foreign locations (including all vessel and

any Tanker Airlift Control Element (TALCE) support) with less than 300 personnel.

TAB B TO APPENDIX 9 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
FIRST RESPONDER MINIMUM REQUIREMENTS (U)

1. (U) General Information. USNORTHCOM First Responder Minimum Requirements. DoD installations, regardless of size, should have some basic level of CBRNE emergency response capability and support. This capability could be organic or provided by local or host-nation agencies.

Levels of Response Capability Guidelines

Responder Level	Objective Response Capability	Associated Equipment	Supporting Training Courses
Awareness Level	• Self protective measures • Protect general population from further contamination	• IPE to include; equipment, detection, and decon capabilities as appropriate	• Responder Awareness Course • Awareness Level all disciplines (except firefighters- minimum is operations level) • Command and Staff Workshop

Operations Level	**Basic competency plus:** • Operate with Hazmat Teams (defensive only) • Initial detection and monitoring (defensive, not in hot or warm zone) • Establish mass casualty response/treatment systems • Establish transport for mass casualties (gross decontamination only) • Implement evacuation plans • Advanced PPE Measures (only if trained) • Conduct operations in a contaminated environment	• Moderate increase level equipment • Level A, B, C PPE • Self Contained Breathing Apparatus (SCBA) • Decontamination • Detection	• Operations Level for Fire and selected Security, EMS, Public Works, physician, nurse, and public health personnel • Technicians for Hazmat or personnel who plan to work in the hot zone • CBRNE Installation Emergency Response Trainers Training & Installation Planners Training
HAZMAT Technician Level	**Operator's competency plus:** • Ability to operate unhindered by equipment shortfalls in any contaminated environment (operators should possess needed equipment to perform tasks) • Conduct safe sampling procedures in contaminated environment	• High –Level Equipment Advanced detection • Computer database references • Computer programming for detection equipment • Responder protected detection equipment	• Technician/Specialist level Hazmat (offensive/hot zone) • Specialist level Physician, Nurse, and Public Health • Emergency Assessment and Detection training

2. (U) Personal protective equipment will be provided in the following order:

a. (U) Emergency Responders. Personnel who work closest to known or suspected CBRN hazards (e.g., emergency responders) should be given the best protection (e.g., “Level A”). In today’s uncertain environment, responders should use maximum possible protection until determined otherwise by competent authority.

b. (U) Critical Personnel. Personnel deemed essential to the performance of critical military missions (whether military, civilian, contractor, Host-nation personnel or third country nationals) should be provided an appropriate level of protection to support continuity of those critical military missions. Since critical missions should be continued without interruption, collective or individual protection may be necessary to sustain critical missions.

c. (U) Essential Personnel. Personnel deemed essential to the performance of essential military operations (whether military, civilian, contractor, host nation personnel or third country nationals) should be provided an appropriate level of protection to support near continuity for those essential military operations. Since essential operations may be interrupted for relatively short periods (i.e., hours to days), escape protection may be necessary to sustain essential operations (i.e., escape, survive, and restore essential operations).

d. (U) Other Personnel. For all other persons not in the above categories, the objective will be to provide the procedures or protection necessary to safely survive an incident. Evacuation procedures, for example, may fulfill this requirement.

e. (U) Included as part of the above categories are those who work or live on DoD installations worldwide, family members authorized overseas, and DoD Contractors if designated in contract agreements and designated as essential to perform critical DoD missions.

TAB C TO APPENDIX 9 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
INSTALLATION CBRNE PROTECTION TRAINING AND EXERCISES (U)

1. (U) General Information. All DoD Elements shall conduct installation CBRNE exercises annually using realistic CBRNE scenarios appropriate to installation mission and vulnerabilities to validate CBRNE training and the concept of operations described in their emergency response plans. CBRNE protection training and exercises shall be integrated into AT training and exercises, plus CBRNE protection shortfalls shall be identified at the same time as AT shortfalls. To incorporate lessons learned, commanders should maintain exercise documentation for at least three years. DoD Elements shall apply these guidelines to installation CBRNE training and exercises.

2. (U) Training Requirements.

a. (U) Installation AT/FP working groups/committees are responsible for planning, assessing, training, and exercising installation CBRNE programs.

b. (U) Ensure all individuals and teams will be trained on the proper use and maintenance of their Personal Protective Equipment (PPE). PPE must be sufficient to provide immediate protection for first-responders, security forces and follow-on support. Shortfalls and additional requirements must be identified and forwarded through command channels for resolution.

c. U) Exercises should include participants from all CBRNE emergency response functions on the installation and whenever possible, appropriate local, State, federal, and host-nation CBRNE participants.

d. (U) Participating in local community CBRNE exercise and training and, where appropriate, local community participation in installation/base CBRNE exercise and training should improve interoperability on installations with local communities (to include other area installations).

e. (U) When possible, the DoD Elements are encouraged to align their installation CBRNE exercise and training schedules with that of DoJ, the Office of Domestic Preparedness exercise and training programs for State and local preparedness programs to include WMD Civil Support Teams (CSTs), as appropriate.

f. (U) As appropriate, support installation CBRNE training and exercises with adequate and appropriate programming, planning, personnel, and funding.

g. (U) Ensure training readiness is achieved once all assigned and attached personnel, units, organizations, and family members are aware of the CBRNE threat; trained to identify and respond to those threats, and have exercised contingency plans which include the CBRNE threat. CBRNE emergency response training sustainment should include mechanisms to train new installation emergency responders.

3. (U) Emergency Response.

a. (U) A CBRNE emergency response training program should be developed and conducted on each installation by the Emergency Disaster Preparedness Officer or the installation Commander's designated person. This training should include appropriate standards and TTP IAW DoDI 2000.18.

b. U) First Responders normally conduct agent identification in a CBRNE incident. For installations/facilities that have a first responder capability, CBRNE emergency response training must include agent identification, detection equipment training, and training in personal protective equipment.

c. (U) Services should incorporate CBRNE emergency response training into curriculum of the schools and other forms of professional military education.

d. (U) CBRNE emergency response training should comply with applicable requirements of 29 CFR 1910.120; National Fire Protection Association Consensus Standard (NFPA) 472, "Standard for Professional Competence of Responders to Hazardous Materials Incidents"; National Fire Protection Association Consensus Standard (NFPA) 473, "Standard for Competencies for EMS Personnel Responding to Hazardous Materials Incidents"; and the appropriate governing Federal, State, or host-nation regulations governing pre-hospital care providers (emergency medical services operations), both Basic Life Support and Advanced Life Support emergency medical services. As applicable, hospital care providers and medical practitioners, should comply with the Joint Commission on Accreditation of Health Care Organizations standards and the Commission on Accreditation of Air Medical Transport.

e. (U) Incorporate lessons learned from installation emergency response CBRNE exercises into existing overall installation FP plans.

4. (U) Emergency Operations Center (EOC). Exercises to test the emergency operations plans for CBRNE events should be complementary to the AT assessment program and not viewed as a separate entity. These should take place often and use a full spectrum of inserts based on realistic threat assessments

5. (U) Medical Response. Conduct Medical Response and IM exercises regularly to test the plan and assess the command's ability to respond to the threat entity use of CBRNE, and conventional munitions.

a. (U) Medical responders must receive adequate CBRNE equipment and training certification necessary to protect themselves and treat casualties.

b. (U) Adequate hospital planning and support capable of treating mass casualties, to include contaminated casualties, is available.

c. (U) Medical mass casualty (MASCAL) and CBRNE scenarios are included in the FP Exercise Program and annual AT exercise.

APPENDIX 10 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
CRITICAL INFRASTRUCTURE PROTECTION (U)

(U) References: *Base Order*

a. (U) DoD Directive 3020, Defense Critical Infrastructure Protection (DCIP) (Draft) (U).

1. (U) Situation. FP is one of Commander, USNORTHCOM's critical capabilities and top ten strategic priorities. USNORTHCOM views FP as the overarching umbrella which includes CIP, AT, installation CBRNE, and IO. It is derived from DoD policy guidance, specifically DoDD 2000.12, DoDI 2000.16, and additional guidance as provided in *ref. a*. Defense Critical Infrastructure (DCI) includes both DoD and non-DoD assets and infrastructures essential to military operations on a global basis. For USNORTHCOM, CIP is integrated with the FP mission. Threats and hazards to critical infrastructure can come from a variety of sources across a full spectrum of activities. These threats include, but are not limited to, traditional physical attack, cyber intrusions, as well as natural hazards such as adverse weather events.

a. (U) Purpose. For USNORTHCOM, CIP is integrated in the FP mission and executed from an all-hazards perspective. This Appendix describes the manner in which CIP is integrated with AT activities within the USNORTHCOM AOR.

2. (U) Mission. *Base Order*.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) The CIP construct consists of the following elements: analysis/assessment of critical asset and infrastructure vulnerabilities, remediation, monitoring and reporting, indications and warning, mitigation, response and reconstitution. Before an attack, incident or event, AOR CIP activities focus on analysis/assessment (e.g., identification, prioritization, assessment of DoD and related assets and infrastructures) and remediation, and monitoring and reporting. Analysis and assessment facilitates the development of FP priorities and recommendations for Courses of Action (COA). Analysis and assessment is likewise critical to mitigation and remediation planning. Due to the interdependent nature of DCI, as well as the number of vulnerabilities, CIP planning requires use of a complex risk management approach integrating efforts across the DoD and civil sectors. An effective risk management methodology enables decision-makers through consideration of a wide range of factors in the process of quantifying the degree of risk.

(2) (U) Methodology. In order to reduce the risk and vulnerability of DoD facilities and assets from full threat spectrum, USNORTHCOM in coordination with other

combatant commands, the military services, the Defense Agencies, DoD Field Activities, and Defense Sector Lead Agencies, will catalog Defense Critical Infrastructure, single points of failure and associated dependencies within the USNORTHCOM AOR essential to accomplishment of objectives in support of the execution the National Military Strategy. Asset identification includes processes to: 1) Identify and document assigned missions (combatant command mission requirements and service missions) and 2) supporting defense critical assets, within the scope of Defense Critical Infrastructure of U.S. military installations, single points of failure and dependencies associated with non-DoD assets. The Joint Staff has taken the lead for the development and implementation of asset identification and prioritization methodologies. The methodology will be consistent with guidance from ASD(HD). When these procedures have been approved, they will be published as a Tab to this Appendix.

(3) (U) Current DoD doctrine specifically requires commanders at all levels to establish an AT Program that defends DoD-owned, -leased, or -managed critical infrastructure and mission essential assets. Although AT is focused on the terrorist threat, the all-hazards approach that USNORTHCOM has adopted under the FP mission umbrella ensures required capabilities under all conditions (i.e., natural disasters, CBRNE). Within the context of the FP mission and AT Program, defense of DoD critical infrastructure is executed under TACON (for FP) authority. Currently, resourcing for remediation/mitigation of critical infrastructure vulnerabilities is accomplished via the various Service/Agency AT Programs within the physical security funding category. Efforts are underway to establish a CIP-specific funding initiative.

(4) (U) The USNORTHCOM methodology for CIP is focused in three Areas: Responsibility, Interest and Influence. An Area of Responsibility is defined as DoD-leased, -owned, and -managed assets/facilities, whereby all commanders (from the Geographic Combatant Commander down to base/installation commanders) have the responsibility to defend critical infrastructure that is leased, owned, or managed by DoD. Second, the Area of Interest includes National-level CIP assets, and consists of a significant amount of critical infrastructure, which are not considered DoD assets, but are critical to sustaining DoD operations (utilities, information networks) that USNORTHCOM must have visibility of. Third, the Area of Influence encompasses the Defense Industrial Base (DIB) and is critical how Commanders at all levels interface with Department of Homeland Security and civilian counterparts.

b. (U) Tasks.

(1) (U) USNORTHCOM will:

(a) (U) Exercise overall responsibility to defend, prevent loss or mitigate loss of DoD-owned critical assets within the USNORTHCOM AOR under the authority of TACON (for FP).

(b) (U) Identify, prioritize, assess and coordinate for the defense of critical infrastructure within the USNORTHCOM AOR.

(c) (U) Produce consolidated USNORTHCOM-prioritized CIP list(s) NLT 01 January each year. This list must encompass facilities/assets critical to USNORTHCOM Mission Assurance, which includes all DoD-owned, -operated or -leased facilities, non-DoD facilities/assets, and DIB facilities/assets within the USNORTHCOM AOR.

(d) (U) Ensure information/intelligence requirements address CIP-specific issues.

(e) (U) Develop a process that rapidly identifies if a threat is directed towards a critical facility or asset. *Appendix 1, Information/Intelligence Flow*.

(f) (U) Coordinate and partner with DoD and non-DoD Elements regarding CIP.

(g) (U) Coordinate with Combatant Commands, DCMA, DHS, and COMs (OCONUS) to identify DIB, Critical Infrastructure Vulnerability Assessments (CI/VA) of DIB, and prioritization of DIB.

(h) (U) Coordinate with DoD Elements to conduct criticality assessments of Critical Infrastructure and interdependencies in the USNORTHCOM AOR.

(i) (U) Ensure CIP is addressed in all appropriate policies, plans, orders and exercises.

(j) (U) Establish comprehensive USNORTHCOM CIP plans, policies and procedures that include specific prescriptive standards to address threat capabilities and geographic settings as it pertains to DoD infrastructure and USNORTHCOM mission accomplishments.

(k) (U) Incorporate CIP assessments standards in USNORTHCOM program reviews and vulnerability assessment program.

(l) (U) Identify, document, validate, prioritize and submit to the Joint Staff resource requirements necessary to ensure the protection, prevention or mitigation of loss of DoD critical infrastructure.

(m) (U) Coordinate remediation risk measures to reflect USNORTHCOM's strategic/operational vice tactical role.

(n) (U) Obtain data and maintain visibility of DIB critical infrastructure.

(o) (U) Ensure CIP requirements are addressed in information architecture requirements and development. Advocate and use Geospatial capabilities and applications.

(p) (U) Coordinate and, where appropriate, perform, annual installation level CI/VA IAW CI/VA format TBP. Results of assessment will be published within 30 days. Results will be reported on CVAMP or similar IT architecture within 30 days of receipt.

(q) (U) Identify and assess critical assets and associated infrastructure dependencies within the USNORTHCOM AOR necessary to assure the availability of networked assets critical to DoD missions.

(r) (U) In coordination with the DoD Elements in the USNORTHCOM AOR, identify and assess critical assets and associated infrastructure dependencies.

(s) (U) (U) Include CIP issues in the USNORTHCOM monthly FP update. *Annex R, Reports.*

(2) (U) DoD Elements will:

(a) (U) Provide USNORTHCOM a consolidated and prioritized list of Critical Infrastructures NLT 01 October each year. It must encompass facilities/assets critical to Mission Assurance, which includes all DoD-owned, -managed or -leased facilities. This list must be in Excel in a standardized, columnar format with headings in the following order: Mission, Mission Required Asset, Mission Supporting Asset, Infrastructure Supporting Asset, Function, Owner, Installation/Facility, Location Lat/Long, Dependencies, Recovery Time (Days), National Critical Asset, Strategic Critical Asset, Operational Critical Asset, and Tactical Critical Asset.

(b) (U) Pass information and intelligence regarding critical infrastructure through existing information/intelligence reporting channels/requirements. *Appendix 1, Information/Intelligence Flow.*

(c) (U) Per DoD policy and mission requirements, coordinate and partner with Federal, State and local authorities regarding CIP.

(d) (U) Address CIP in all operational plans, orders and exercises to ensure critical capabilities are maintained, as outlined in CJCSM 3122.03A Joint Operating Planning and Execution System (JOPES) Volume II Planning Formats and Guidance, Annex C Appendix 16, 31 Dec 1999, change 1 to 06 Sept 2000.

(e) (U) CIP exercise issues should be outlined in an After Action Report (AAR) and forwarded to USNORTHCOM.

(f) (U) Develop a comprehensive program to identify, prioritize, assess, manage risk and provide for remediation and mitigation of vulnerabilities of DoD critical infrastructure.

(g) (U) Develop a comprehensive program to identify, prioritize, assess and manage risk for non-DoD critical assets and infrastructure.

(h) (U) Develop AT Physical Security Plans that integrate facilities, equipment, personnel and procedures to maximize protection of personnel and assets.

(i) (U) Provide for remediation and mitigation of vulnerabilities for DoD critical infrastructure.

(j) (U) Conduct an annual VA on all critical infrastructure. This assessment must include the identification and mitigation of interdependences and single points of failure. All assessments will be provided to USNORTHCOM Assessment Branch and loaded in CVAMP.

(k) (U) Identify, document, validate, prioritize and submit to USNORTHCOM resource requirements necessary to ensure the protection, prevention or mitigation of loss of critical infrastructure. PPBE submission and CbT RIF are outlined in Annex C, Appendix 7. Efforts are underway to establish a CIP specific funding initiative.

(l) (U) DCMA will annually provide USNORTHCOM with a consolidated DIB critical infrastructure list.

(m) (U) Identified CIP vulnerabilities must be included for resource and requirements inputs for funding.

(n) (U) Establish, resource and execute an organizational CIP program that supports USNORTHCOM mission essential CIP tasks and capabilities. Efforts are underway to establish a CIP specific funding initiative.

(o) (U) Address Top 3 CIP issues in DoD Element monthly FP update. *Annex R, Reports.*

(p) (U) Provide USNORTHCOM with:

1. (U) Tasking POCs for their CIP program offices.

2. (U) 24-hour operations center contact information, or 24-hour POC if no operations center is available.

3. (U) Information necessary for NC/J34 to establish accounts/passwords for access to the website/restricted portal.

4. (U) Ensure all information is current/updated on a monthly basis.

APPENDIX 11 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
RULES OF ENGAGEMENT AND USE OF FORCE POLICY (U)

(U) References: *Base Order.*

a. (U) DoD Directive 5210.56, Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties, November 1, 2002 (Change 1, January 24, 2002).

1. (U) Situation.

a. (U) Purpose. This appendix provides guidance for the arming of personnel for whom Commander, USNORTHCOM, has been given responsibility for FP. It is based on guidance in Enclosure 1 to ref. a. It establishes command policy and delegates authority to approve the carrying of firearms outside US/DoD-controlled compounds in the USNORTHCOM AOR for personal protection, for protective armed escort or convoy duty, and for transport between billeting and place of duty. This policy further clarifies weapons issued in conjunction with approved exercises or military operations. This appendix provides additional guidance on use of force for personnel performing law enforcement or security functions.

2. (U) Mission. *Base Order*.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) Rules of Engagement (ROE). For U.S. territories and possessions within the USNORTHCOM AOR, ref. a. applies.

(2) (U) Arming Policy.

(a) (U) General. Arming policy for law enforcement, security purposes, or personal protection varies by assignment or status of the personnel or unit performing duty in CONUS.

1. (U) Requirements. Before any individual is issued a firearm for law enforcement, security purposes, or personal protection, that individual must be qualified IAW service requirements on assigned individual and/or crew served weapons, as appropriate, and fully trained on the applicable rules for the use of deadly force.

a. (U) If assigned or issued individual weapon(s), personnel will conduct battlesight zero (if applicable to that weapon, e.g. M-16) and qualify on the weapon before assignment in the USNORTHCOM AOR. Maintenance on individual weapons will be performed in accordance with service regulations.

b. (U) Personnel will maintain qualification standards IAW Service requirements. Training records will be maintained by the unit/activity.

2. (U) Coordination. Commanders will advise the NC/J34 and the appropriate USDR of all instances where the issuance of firearms has been authorized. Notification will be as soon as possible but not longer than 24 hours after such authorization. NC/J34 will seek consistency among the Services in the application of this policy and ensure required coordination with the COMs per DoD and DoS MOUs on FP on Security of DoD Elements and Personnel in Foreign Areas.

(b) (U) Contingency Operations. Operations in support of a specific mission or execution of an OPORD/OPLAN (may be in PCS or Temporary Duty Status). Guidance provided for specific contingency operations supersedes this operating instruction.

1. (U) In determining the necessity to issue firearms, Commanders will use the guidance provided for the mission and weigh the potential of the threat in the particular location, the adequacy of protection by the government (local through national) authorities, and the effectiveness of other active and passive means. Before issuing a firearm to an individual for personal protection or providing an individual an armed security detail, due regard must be given to the individual‘s rank, position, duties and overall profile as a likely target of a terrorist attack.

2. (U) Personnel in the USNORTHCOM AOR for whom the Commander, USNORTHCOM has TACON (for FP) responsibility will not routinely carry firearms off DoD facilities. Commanders may authorize U.S. forces under their command to carry firearms between billeting areas and assigned duty locations when there is no weapon storage facility available at that location. Additionally, under exceptional circumstances, they may authorize selected individuals to carry firearms for personal protection or for providing protective armed escort or convoy duty.

3. (U) Authorization to carry firearms off DoD-controlled compounds for personal protection, armed escort, or transport between billeting and place of duty will be given only on a case-by-case basis for a specified assignment or period of time.

(c) (U) Unit Deployments. Deployments for the purpose of exercises, training, or humanitarian missions in support of USNORTHCOM or a COM.

1. (U) Units deploying to the USNORTHCOM AOR for exercises and training may deploy with their weapons. The availability of weapons while deployed will be based on the following (2) two stages:

a. (U) Stage I. Weapons and ammo stored and secured by the Unit Commander.

b. (U) Stage II. Weapons and ammo issued to unit personnel.

2. (U) This policy allows Commander, USNORTHCOM to provide for the personal security of deployed units and respond to changes in threat conditions. This policy also allows for a redeployment of the unit should a situation in the USNORTHCOM AOR change. The term unit is used here to denote an organization or a portion of an organization that can be reconstituted and redeployed to support a contingency operation or major theater war.

(d) (U) Temporary Duty. In support of USNORTHCOM missions (e.g., conferences, coordination, orientation, etc.).

1. (U) Personnel traveling in the USNORTHCOM AOR for other than contingency operations or unit deployments normally do not require arming.

2. (U) When there is a reasonable expectation that life or DoD assets will be jeopardized if firearms are not carried, authorization to carry firearms may be issued to qualified personnel in accordance with the procedures provided for in ref a.

(e) (U) Contract Guards. This arming policy does not pertain to contract security personnel who perform duties IAW contracts or agreements. Such documents must be consulted for guidance on arming of these personnel.
(See paragraph 3.d. below regarding use of deadly force criteria. These criteria apply to contract security forces as well as DoD personnel.)

(3) (U) Use of Force.

(a) (U) General.

1. (U) This policy applies to personnel assigned to or performing security duties (to include FP and AT duties) in the USNORTHCOM AOR.

2. (U) This policy does not apply to personnel engaged in combat activities or similar military operations subject to authorized supplemental ROE or assigned to duty in a combat zone in time of war, in a designated hostile fire area when ROE apply, or when Commander, USNORTHCOM issues orders setting forth different criteria.

(b) (U) Policy.

1. (U) Personnel will not be permitted to perform security duties requiring the use of weapons until they have received instruction IAW ref a., and other applicable procedures or guidance that may be established by subordinate Commanders for the use of force in the performance of such duties.

2. (U) Personnel engaged in or security duties will avoid the use of force where they can carry out their duties without resorting to its use. In cases where the

use of force is warranted, DoD law enforcement and security personnel will use the minimum amount of force necessary to achieve their objective.

(c) (U) Additional Requirements for the Use of Firearms.

1. (U) In the case of holstered weapons, a weapon should not be removed from the holster unless there is a reasonable expectation that use of the weapon may be necessary.

2. (U) Warning shots are prohibited except as authorized by the SecDef within U.S. territorial seas and internal waters on 16 May 03 in CFFC Implementing Message dated 011647z Aug 03. Warning shots are authorized within U.S. territorial seas and internal waters under these specific conditions:

a. (U) Warning shots to protect Navy vessels and Naval Service vessels within territorial seas and internal waters of the United States are authorized in the appropriate exercise of FP of Navy and Naval Service vessels, they are fired:

1) (U) Over water to warn an approaching vessel;

2) (U) When a clear line of fire exists;

3) (U) From an approved rifle or a crew-served weapon;

4) (U) By qualified and certified personnel;

5) (U) Under tactical direction of competent authority; and

6) (U) When there are no other means reasonably available to determine the intent of the approaching craft without increasing the threat to the Navy and Naval Service vessel or personnel.

3. (U) Shots will be fired only with due regard for the safety of innocent bystanders.

4. (U) When a firearm is discharged, it will be fired with the intent of rendering the person(s) at whom it is discharged incapable of continuing the activity or course of behavior that prompted the individual to shoot.

5. (U) Subordinate commanders may impose further restrictions on the use of firearms if deemed necessary in their judgment and if such restrictions would not unduly compromise the national security interests of the US.

(d) (U) Use of Deadly Force. See *ref. a*.

APPENDIX 12 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
INFORMATION OPERATIONS (U)

(U) References:

a. (U) DEPSECDEF MEMO on OPSEC 6 June 2003

b. (U) Joint Pub 3-13, 9 October 1998, “Joint Doctrine for Information Operations”

c. (U) Joint Pub 3-13 (Classified Appendix), 9 October 1998, “Appendix A to Joint Doctrine for Information Operations Policy”

d. (U) Joint Pub 3-13.1, 7 February 1996, “Joint Doctrine for Command and Control Warfare (C2W)”

e. (U) Joint Pub 3-51, 7 April 2000, “Joint Doctrine for Electronic Warfare”

f. (U) Joint Pub 3-53, 10 July 1996, “Doctrine for Joint Psychological Operations”

g. (U) Joint Pub 3-54, 24 January 1997, “Joint Doctrine for Operations Security”

h. (U) Joint Pub 3-58, 31 May 1996, “Joint Doctrine for Military Deception”

i. (U) Joint Pub 3-61, 14 May 1997, “Doctrine for Public Affairs in Joint Operations”

j. (U) DoD Directive 0-8530.1, 8 January 2001, “Computer Network Defense (CND)”

k. (U) DoD Directive S3600.1, 9 December 1996, “Information Operations”

l. (U) CJCS Instruction 3110.05B, 15 June 1999, “Joint Psychological Operations Supplement to the Joint Strategic Capabilities Plan FY 1998”

m. (U) CJCS Instruction 3210.01A, 6 November 1998, “Joint Information Operations Warfare Policy”

n. (U) CJCS Instruction 3210.03B, 31 July 2002, “Joint Electronic Warfare Policy”

o. (U) CJCS Instruction 3211.01B, 2 January 1998, “Joint Policy for Military Deception”

p. (U) CJCS Instruction 3213.01A, 1 December 1997, “Joint Operations Security”

q. (U) CJCS Instruction 6510.01C, 1 May 2001, “Information Assurance and Computer Network Defense”

r. (U) CM 510-99, 10 March 1999, “Information Operations Conditions”

s. ASD(C3I) Memorandum, 26 February 2003, “Guidance for Computer Network Defense Response Action”

t. (U) NORAD/NORTHCOM Instruction 10-100 (U)

(U) General. This appendix provides guidance for the use of Information Operations as an integral part of Force Protection (FP) and in support of all other FP activities, including AT training and countermeasures. This tab separates and discusses IO that is unique to FP or requires highlighting when planning FP. IO are covered in depth in Appendix 3, to Annex C to USNORTHCOM CONPLAN 2002.

a. (U) FP includes many IO aspects. For the purposes of this appendix, they will be referred to as FP Information Operations (FPIO). FPIO includes, but is not limited to the traditional defensive IO capabilities of Operations Security (OPSEC) and Computer Network Defense (CND). Strategic Communications, a related activity, is important to FP although DoD’s role is to provide a component of the overall U.S. Government Strategic Communications plan to deliver messages to an adversary, including the leadership of terrorist organizations. Other IO capabilities such as tactical Military Deception and Electronic Warfare have potential for FP, but their use is threat and scenario dependent. The supporting capability of Public Affairs is important to the overall FP effort and is discussed at Annex F.

b. (U) OPSEC, including Communications Security (COMSEC), Information Security (INFOSEC), Computer Security (COMPSEC), when combined with Physical Security, will be key to the success of any FP effort. OPSEC, unlike traditional security programs specifically designed to protect classified information, is concerned with identifying, controlling, and protecting generally unclassified information associated with sensitive operations and activities. However, OPSEC and designated classified security programs must work in conjunction with one another to ensure all aspects of operations are protected. OPSEC is a command responsibility. At each level of command, the operations officer, or his equivalent, is responsible to the commander for coordinating overall OPSEC planning. Each headquarters preparing a supporting plan will appoint an OPSEC officer to ensure OPSEC considerations are effectively carried out. Each and every individual in every command assists in safeguarding the security of operations and is responsible for ensuring that the “need to know” is rigorously applied at all times.

1. (U) Situation.

a. (U) Enemy Forces. For specific threats, see Annex B.

b. (U) Friendly Forces. See Base Order.

2. (U) Mission. See Base Order.

3. (U) Execution.

a. (U) Concept of Operations.

(1) (U) OPSEC.

(a) (U) OPSEC and Physical Security are the most important components of FP.

(b) (U) OPSEC is a command function.

(c) (U) An emphasis on OPSEC and the employment of OPSEC monitoring indicators such as COMSEC and Counterintelligence (CI) assesments are important to an effective OPSEC program.

(d) (U) Most friendly force vulnerabilities to tactical reconnaisance can be identified and a program designed to frustrate tactical intelligence collection, including some camouflage of DoD protection operations against surveillance.

(2) (U) Computer Network Defense (CND). Commanders shall:

(a) (U) Develop an efffective integrated cyber defense plan to ensure Information Assurance (IA) can be based upon local defenses such as continuous system administrator training, implementation of all Information Assurance Vulnerability Assessment (IAVA) bulletins, and employing the latest version of IA software for Intrusion Detection Systems (IDS) and firewalls.

(b) (U) Evaluate the physical vulnerability of cyber critical infrastructure required to ensure IA. See Appendix 10 to Annex C.

(c) (U) Train personnel to practice good computer security, which serves to frustrate most cyber intrusions attempts.

(3) (U) Electronic Warfare.

(a) (U) While scenario-dependent, an effective FP Plan will include the possible use of capabilities provided by Electronic Protect (EP) , Electronic Support (ES) and Electronic Attack (EA).

(b) The use of EA assets will require coordination with higher authority and the Federal Communications Commission (FCC).

(4) (U) Tactical Military Deceoption.

(a) (U) Depending on warning time and the depth of threat intelligence, Military Deception (MILDEC) can enhance other force protection applications and create a need to delay for a potential attacker to conduct further tactical reconnaissance to ascertain the actual tactical conditions.

(b) (U) OPSEC is absolutely required to support Operational Deception.

(c) (U) Deception can never use the media or command public affairs personnel as part of the deception.

(d) (U) Tactical deception must be vetted with the Command Judge Advocate.

(5) (U) Strategic Communcication.

(a) (U) The Joint Staff Definition of Strategic Communication is "*The transmission of integrated and coordinated U.S. Government themes and messages that advance U.S. interests and policies through a synchronized interagency effort supported by public diplomacy, public affairs, and military information operations, in concert with other political, economic, information, and military actions*."

1. (U) The concept of Strategic Communication is part of FP.

2. (U) Local DoD announcements and actions must support the overall Government message.

b. (U) Tasks.

(1) (U) Intelligence Support.

(a) (U) Monitor hostile intelligence threats.

(b) (U) Analyze threat collection capabilities and intentions.

(c) (U) Analyze the adversary/terrorist information needs to assist NC/J3 in developing essential elements of friendly information (EEFI).

(d) (U) Identify friendly force vulnerabilities to intelligence collection (to include trash bin diving and open source intelligence), terrorism, and sabotage.

(e) Forward cyber threat data from the Intelligence Community (IC), Joint Task Force Global Network Operations (JTF_GNO) and USSTRATCOM'S Joint Force Component Commander-Network Warfare (JFCC-NW).

(f) (U) Provide techinical threat data to support the use of EW assets,if possible.

(g) (U) Assist in developing force profiles.

(h) (U) Assist in developing adversary leadership profiles and modus operandi to support tactical military deception planning.

(i) (U) Provide input to and review deception and other plans as necessary.

(j) Coordinate reporting CI/AT/LE activities within USNORTHCOM AOR that may impact this plan.

(2) (U) USNORTHCOM Director of Operations.

(a) (U) Direct the use of all IO capabilities by local commanders to support AT/FP planning and execution, as appropriate to the FPCON and threat intelligence.

(b) (U) Support local commanders planning and operational requirements, when required by the current threat stream, for IO capabilities outside the local command.

(3) (U) Local Commanders.

(a) Compile a list of EEFI and identify information critical to success of the FP mission.

(b) (U) Develop an integrated local cyber defense plan.

(c) Consider the use of tactical electronic warfare assets, camouflage and tactical military deception to confound an attack. See Appendix 11, Rules of Engagement.

c. (U) Coordinating Instructions.

(1) (U) Ensure OPSEC is integrated into training, operations and plans.

(2) (U) Ensure OPSEC plan addresses necessary C2 protection and is coordinated with CNO, EW and tactical MILDEC.

(3) (U) All DoD personnel have responsibility to avoid discussing sensitive but unclassifed information as well as classifiied information, critical information, or EEFI with personnel not having proper security clearances and a need-to-know.

4. (U) Logistics.

a. (U) In accordance with Annex C, Appendix 8.

5. (U) Command and Control.

a. (U) Command. Commander, USNORTHCOM has the responsibility for directing FPCON and their implementation. See Appendix 5 to this Annex.

b. (U) Feedback. *Annex R, Reports*.

APPENDIX 13 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
FORCE HEALTH PROTECTION (U)

(U) References: *Base Order*.

1. (U) Situation.

a. (U) Purpose. To provide guidance for the execution and oversight of USNORTHCOM Force Health Protection (FHP) as it applies to the AT Program. FHP is a command responsibility at all levels. FHP is a focus on healthcare programs that protect American's fighting forces. FHP is a "total life-cycle" health support system supporting the concepts described in the Joint Vision through an integrated and focused approach to protect and sustain DoD's most important resource: its Service members and their families – throughout the entire length of service commitment. As such, FHP is a critical component of AT.

2. (U) Mission. *Base Order.*

3. (U) Execution. This Appendix applies to all units operating in the USNORTHCOM AOR and subordinate USNORTHCOM joint activities, to include USDRs, Direct Reporting Units (DRU), and Combined/Joint Task Forces (CTF/JTF).

a. (U) Tasks.

(1) (U) Commanders will:

(a) (U) Ensure all U.S. military personnel receive required immunizations and follow prescribed preventive medicine guidance and procedures.

(b) (U) Ensure health service support is integrated into their AT plan, to include mass casualty planning, WMD identification and risk management, food and water VAs, and other appropriate preventive medicine measures.

(c) (U) Incorporate health service support requirements into AT Program PPBE and CbT RIF funding processes IAW the procedures established in Appendix 7 to Annex C.

(2) (U) NORAD-USNORTHCOM Command Surgeon (SG) will:

(a) (U) Coordinate health service support, including medical response to mass casualty situations, strategic patient movement and definitive medical treatment for any actual terrorist incident.

(b) (U) Promulgate FHP guidance for the areas in which USNORTHCOM has FP responsibility.

(c) (U) Provide subject matter experts to form USNORTHCOM HHQ VA teams.

(d) (U) Publish FHP and Preventive Medicine measures information on the USNORTHCOM Surgeon's web page [NIPRNet: https://www.noradnorthcom.mil/SG/].

(e) (U) Distribute health-related indications and warnings IAW the procedures established in Appendix 1 to Annex C of this order.

APPENDIX 16 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
USNORTHCOM STAFF TASKS (U)

(U) References: *Base Order*.

1. (U) Situation.

a. (U) Purpose. To provide guidance for the USNORTHCOM Staff as it applies to the AT Program.

2. (U) Mission. *Base Order.*

3. (U) Execution.

a. (U) Tasks.

(1) (U) N-NC/J1 will:

(a) (U) In coordination with the assigned and Supporting Command Personnel Directorates, ensure all PCS, TDY or TAD orders for personnel stationed or temporarily in the USNORTHCOM AOR indicate the requirement for Level I AT training. USNORTHCOM will determine DoD Element compliance using HHQs program assessments.

(b) (U) Require TDY/TAD orders to specify the authority responsible for security: Commander, USNORTHCOM as well as the local AT POC for personnel TDY/TAD within the USNORTHCOM AOR.

(2) (U) N-NC/J2. Overall Staff lead for execution of Information/Intelligence Flow tasks. Critical sub-tasks include:

(a) (U) Provide Information on Terrorist Activities, Trends and Indicators.

1. (U) Ensure effective application of the Terrorism Threat Level classification system for an integrated terrorism threat analysis, incorporating information collection and analysis from all sources.

2. (U) Ensure that a capability exists to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack. Develop the capability to fuse suspicious activity reports from military security, law enforcement, and counterintelligence (CI) organizations with national-level intelligence, surveillance, and reconnaissance collection activities.

3. (U) Coordinate with CIFA who shall maintain a domestic law enforcement database that includes information related to potential terrorist threats directed against DoD.

4. (U) Keep subordinate Commanders informed of the nature and degree of the threat. Ensure that Commanders are prepared to respond to changes in threats and local security circumstances. Ensure that the Chiefs of Mission (COM) are fully and currently informed of any threat information relating to the security of those DoD Elements and personnel under their security responsibility, but not under the command of the Combatant Commander.

(b) (U) Provide Terrorist Threat Assessments.

1. (U) Produce a terrorist threat assessment at least annually for the command and identify the full range of known or estimated terrorist capabilities for:

a. (U) Counterterrorism Tiers 0 through 2 transnational terrorist organizations as defined by the Interagency Intelligence Committee on Terrorism.

b. (U) Domestic groups operating in the USNORTHCOM AOR intent on attacking DoD interests.

2. (U) Provide threat assessments upon request from NC/J34 in support of Threat and Vulnerability Assessment Products (TVAPs) for National Security Special Events (NSSEs) and other special events. *Annex C, Appendix 6*.

3. (U) Provide to NC/J34, in coordination with DIA and other external intelligence community agencies and organizations, terrorist threat assessments produced by JITF-CT, TTIC, DHS, and the IICT relevant to USNORTHCOM's AOR.

4. (U) Submit NC/J34 intelligence requirements into COLISEUM.

5. (U) Disseminate FP intelligence products through the N-NC/J2 SIPRNet website as well as through intelligence channels to DoD Elements.

(c) (U) Provide a Terrorist WMD Threat Assessment.

1. (U) Provide to NC/J34, in coordination with NC/J34 CBRNE subject matter experts, DIA and other external intelligence community agencies and organizations, an annual WMD threat assessment relevant to USNORTHCOM's AOR.

2. (U) Submit NC/J34 intelligence requirements into COLISEUM.

3. (U) Disseminate FP intelligence products through the N-NC/J2 SIPRNet website as well as through intelligence channels to DoD Elements.

(d) (U) Participate in a Continuous Threat Analysis Process.

1. (U) Participate in the Threat Working Group (TWG) and provide any available intelligence (i.e., SIGINT, LE reports, TALON, etc.) that may indicate a specific threat is imminent in the USNORTHCOM AOR. Information will be passed in the most efficient method possible. N-NC/J2 will provide the TWG with real-time threat assessments, link-analysis and trends pertaining to the specific threat, and predictive analysis of the specific threat.

2. (U) Participate in the Force Protection Action Officer (FPAO) group and provide updates on current/emerging threats.

3. (U) Provide to NC/J34, in coordination with CIFA, trend analysis data on suspicious incident reporting to the FPAO.

4. (U) Provide to NC/J34, in coordination with CIFA, specific correlation analysis of suspicious activities as requested by NC/J34 and present that data at the FPAO.

5. (U) Submit NC/J34 intelligence requirements into COLISEUM.

6. (U) Coordinate with NC/J34 in the Priority Intelligence Request (PIR) process and ensure the process accepts inputs from organizations, divisions or branches outside of N-NC/J2.

7. (U) Disseminate FP intelligence products, to include Defense Terrorism Warning Reports, through the N-NC/J2 NORAD/USNORTHCOM Intelligence Systems (NUIS) and SIPRNet websites as well as through intelligence channels to NC/J34 and DoD Elements.

(e) (U) Provide Country-specific Threat Assessments.

1. (U) Commanders with geographic responsibilities have significant responsibilities for protecting personnel within their AOR. Individuals traveling OCONUS for either permanent or temporary duty will complete annual Level I AT Awareness Training and will receive an AOR-specific update within three months of travel.

2. (U) Provide to NC/J34, in coordination with DIA and other external intelligence community agencies and organization, country-specific threat assessments relevant to the USNORTHCOM AOR. Derivation of the terrorist threat level in a specific country shall be based on the DoD Terrorism Threat Level classification system.

3. (U) Coordinate with and provide to NC/J34 a USNORTHCOM AOR Terrorism Threat Level assessment.

4. (U) Submit NC/J34 intelligence requirements into COLISEUM.

5. (U) Disseminate FP intelligence products through the N-NC/J2 SIPRNet website as well as through intelligence channels to DoD Elements.

(3) (U) NC/J3.

(a) (U) NC/J31. Responsible for integrating USNORTHCOM AT/FP planning and guidance into all NC/J31 planning.

(b) (U) NC/J32. Responsible for all counterterrorism (CT) planning and guidance for the Command's Combating Terrorism (CbT) Program.

1. (U) Act as the Theater Clearance Approval Authority for all personnel assigned or attached to Special Operations assets. NC/J32 will coordinate these theater clearances with NC/J34.

(c) (U) NC/J33/JOC. Serves as the Command's focal point for information flow to include FP information as designated in Annex C, Operations. Maintains the Command's situational awareness (SA) of the USNORTHCOM AOR FPCON status.

(d) (U) NC/J35. Incorporate FP guidance from NC/J34 into all policies, plans, and orders.

(e) (U) NC/J39. In coordination with USSTRATCOM, provides planning expertise and guidance to USNORTHCOM regarding all aspects of Information Operations (IO). Through coordination with USSTRATCOM, NC/J39 provides results of IO assessments to NC/J34.

(4) (U) N-NC/J4. USNORTHCOM Staff lead for execution of logistics support for AT tasks. Responsibilities include:

(a) (U) Plan for and participate in CIP related programs, as well as assist NC/J34 to coordinate and make recommendations on unresolved AT facility requirements during programming and budget reviews.

(b) (U) Establish procedures with the DoD Elements to verify that all AT design construction standards meet the Unified Facilities Criteria (UFC) (*ref. m*).

(c) (U) Coordinate with NC/J34, OSD and the Senior Engineer Working Group (SEWG) to develop specific AT construction deviation request procedures for the USNORTHCOM AOR.

(d) (U) Ensure through the DoD Elements that programs are in place to validate logistics support contracts and agreements to consider AT where applicable.

(5) (U) NC/J5. Incorporate FP guidance from NC/J34 into all USNORTHCOM policies, plans, and orders.

(6) (U) NC/J6. Coordinate with NC/J34 for the inclusion of FP mission considerations into all IT architecture planning.

(7) (U) N-NC/J7. Coordinate with NC/J34 for the inclusion of FP TTP into USNORTHCOM training and exercises.

(8) (U) N-NC/J8. Support USNORTHCOM's AT resourcing efforts for the theater Risk Management program.

(a) (U), N-NC/J8 is responsible for PPBE submissions, in collaboration with NC/J34, for inclusion in the appropriate resourcing venues and products for submission to the Services, Joint Staff, and/or OSD.

(9) (U) N-NC/SG.

(a) (U) Coordinate health service support, including medical response to mass casualty situations, strategic patient movement and definitive medical treatment for any actual terrorist incident.

(b) (U) Promulgate force health protection guidance for the areas in which USNORTHCOM has force protection responsibility.

(c) (U) Provide subject matter experts to form USNORTHCOM HHQ vulnerability assessment teams.

(d) (U) Publish FHP and Preventive Medicine measures information on the USNORTHCOM Surgeon's web page [NIPRNet --https://www.noradnorthcom.mil/SG/].

(10) (U) N-NC/PA.

(a) (U) Coordinate and forward proposed AT public affairs guidance (PAG) to the Assistant Secretary of Defense for Public Affairs (ASD/PA) for Washington-level coordination, approval, and use as appropriate.

(b) (U) Advise USNORTHCOM on all PA issues associated with AT Programs.

(c) (U) Coordinate internal AT information programs and disseminate approved communication themes and talking points.

(d) (U) Provide policy guidance to on-scene PAO personnel during actual or exercise terrorist incidents and delegate release authority to on-scene PAOs as appropriate.

(e) (U) If necessary, in conjunction with an actual terrorist incident, establish a joint information bureau to facilitate public release of information.

(f) (U) Disseminate Travel Restrictions though sub-unified and Component command PAO channels. On a quarterly basis, publish reminders to the command of travel restrictions and AT policies.

ANNEX F TO USNORTHCOM OPORD 05-01 (U)
PUBLIC AFFAIRS (U)

(U) References: *Base Order*.

a. (U) JP 3-61, Doctrine for Public Affairs in Joint Operations

b. (U) CJCS Instruction 3212.01, Joint Operations Security

c. (U) DOD Directive 5122.59, Assistant Secretary of Defense (PA), DOD Principles of Information

d. (U) DOD Directive 5200.1, DOD Information Security Program

e. (U) DOD 5200.1-R, DOD Information Security Program Regulation

f. (U) DOD 5230.9, Clearance of DOD Information for Public Release

g. (U) DOD Instruction 5230.29, Security and Policy Review of DOD Information for Public Release

h. (U) DOD Directive 5400.13, Joint Public Affairs Operations, Unclassified

i. (U) DOD Instruction 5400.14, Procedures for Joint Public Affairs Operations

j. (U) DOD Instruction 5405.3, Development of Proposed Public Affairs Guidance

1. (U) Situation

a. (U) General. This Annex provides general Public Affairs (PA) guidance and instructions to be used by U.S. Northern Command and its supporting units. The Office of the Assistant Secretary of Defense for Public Affairs will issue Public Affairs Guidance related to CONUS Antiterrorism Operations (AT). This guidance will include public affairs posture, strategy, messages and questions and answers for responding to public and media queries.

b. (U) Enemy. See Annex B, Intelligence.

c. (U) Friendly. See Annex A, Task Organization.

d. (U) Policy. Office of the Assistant to the Secretary of Defense for Public Affairs (OASD/PA) policy guidance recommends pursuing a proactive, vigorous public information program consistent with military security considerations to inform the American people. The basic Department of Defense (DoD) Principles of Information will be followed. PA activities are an integral and essential part of military operations.

e. (U) Assumptions. See basic OPORD.

2. (U) Mission. To keep the public (domestic and foreign) informed of U.S. Northern Command's AT mission and overall operations consistent with the constraints of operations security (OPSEC) and information security (INFOSEC).

3. (U) Execution

a. (U) Concept of Operations. U.S. Northern Command PA will provide PA support to the AT effort in direct coordination with OASD/PA and subordinate commands and the DoD Elements, as required.

b. (U) Tasks/Coordinating Instructions

(1) (U) U.S. Northern Command PA is responsible for release of information:

(a) (U) Subordinate commanders may discuss the subject of AT as it pertains to those areas/installations/sites for which they have responsibility. However, discuss AT measures and procedures only in general terms without going into specific details. Do not provide specifics regarding security measures, e.g., "we are inspecting xx% of vehicles," or provide information regarding vulnerabilities, e.g., "our greatest vulnerability is xxxxx."

(b) (U) Incidents of terrorism will generate extreme apprehension and potentially panic in the public. In response to queries concerning a possible or real terrorist threat or action at or near a particular activity, installation, or community, the local commander may acknowledge that increased security measures have been or will be taken without going into specific details regarding the measures being implemented, however it is appropriate and operationally sound to acknowledge the obvious. For example, increased AT measures such as additional guards at the gate and/or more stringent identification checks should be acknowledged and may serve to send a positive message of increased readiness.

(2) (U) DoD Element and Supporting Commands are responsible for:

(a) (U) Being available in an on-call status 24 hours per day for agency and Service-specific support of emergency and contingency operations under this OPORD.

(b) (U) Providing background and other related information support for releases (internal/external), PAG, RTQ, products, etc., as required/tasked.

(c) (U) Coordinating all PA activities and operations with USNORTHCOM PA as appropriate/required.

4. (U) Security of Operations and Personnel

a. (U) Implementing this Annex presents a variety of challenges in maintaining a balance between security and providing unclassified and cleared information to the public. This balance should not preclude providing maximum assistance to media correspondents to support their coverage of the USNORTHCOM AT mission.

b. (U) PA at all levels will ensure that news media representatives (NMRs) are briefed on security issues. Media representatives are responsible for their own personnel security.

5. (U) Operations Security. The purpose of OPSEC is to identify, control and protect critical and sensitive information associated with planning and conducting military operations. Personnel should not begin PA planning without reviewing and consulting their respective classification guides and OPSEC Critical Information Lists (CIL).

6. (U) Audio Visual and Visual Information. Combat Camera (COMCAM) and other audio visual requirements, if required, will be coordinated with USNORTHCOM/PA, and supporting command element PA Offices as required for internal operational, historical and PA internal audio visual support.

7. (U) USNORTHCOM PA Key Telephone Listings and Points of Contact. Chief of Public Affairs (USNORTHCOM/PA), Commercial (719) 554-6889 or DSN 692-6889; After hours contact is via pager (719) 450-0464 or cell phone (719) 330-5169.

TIMOTHY J. KEATING
Admiral, USN
Commander

OFFICIAL

MICHAEL B. PERINI, GS-15
Director of Public Affairs

ANNEX R TO USNORTHCOM OPORD 05-01 (U)
REPORTS (U)

(U) References: *Base Order*.

1. (U) Situation. *Base Order*.

2. (U) Mission. *Base Order*.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) Monthly FP Update Report. Monthly FP Updates will be submitted IAW the following guidance:

(a) (U) FP Update Period. Update period begins on the first day of the month and runs through the last day of the month. The covered update period serves as the identification period when submitting the monthly update (e.g. 1-30 November 04 is the 2004-11 Update).

(b) (U) FP Update Due Date. Updates are due NLT than 2300 ZULU on the 10th day of the month following the reporting month.

(c) (U) FP Update Submission. Submitted via the NC/J34 FP/MA restricted portal by uploading the document into the "Submit Update" area of the J34 Reports/Information Sub-Web (Restricted Access). First priority is to submit via the SIPRNET. Second priority is to submit via the NIPRNET. It is not required to submit on both portals. In the event of document upload failure on the portal, alternate submission may be accomplished via email to the NC/J34 RM organizational mailbox (address located in Tab A to Appendix 1 to Annex C).

(d) (U) FP Update Requirements. Updates containing classified information must have the appropriate classification markings. Provide update in a word document following the paragraph format identified in Figure R-1. Information that has not changed from previous reports may be annotated as "No Change".

MONTHLY FP UPDATE

1. FPCON STATUS UPDATE	Review and identify changes required to the NC J34 FPCON Baseline and Deviation Tracking Document located under the FORCE PROTECTION CONDITIONS area of the J34 webpage; https://www.noradnorthcom.smil.mil/j3/j34/ **PARAGRAPH INFORMATION REQUIRED:** Provide in Update: Affected DoD Element Identity.

	FPCON Level with any higher level measures. DTG Effective or implemented. Remarks which explain why the change occurred and anticipated duration.
2. LONG-TERM DEVIATION UPDATE	Applies to DoD Element FPCON baselines a full level above USNORTHCOMs or installation/activites/offices/locations a full FPCON level above the established FPCON baseline of its command. Conduct review of each deviation every 90 day period that it is in effect and provide details requested below. **PARAGRAPH INFORMATION REQUIRED:** Name of location reviewed, results or findings, and FPCON decision.
3. AT VULNERABILITIES	Identify the top three systemic or across the board AT vulnerabilities within the organization that receive command awareness at the Service/DoD Agency level (macro-level). Functional area topics may range from AT Plans & Programs; Counterintelligence, Law Enforcement, Liaison, & Intelligence Support; AT Physical Security Measures; Vulnerability to a Threat or Terrorist Incident Response Measures; Availability of Resources; Adequacy of Inter-Service/ Agency or Tenant Organizations to enhance force protection measures or respond to a terrorist incident; and others as deemed appropriate. **PARAGRAPH INFORMATION REQUIRED:** Identify the vulnerabilities. Provide amplifying discussion on vulnerability, actions taken to mitigate or eliminate the vulnerability, and any lessons learned or TTP's. Identify the type of assistance required (if any) from USNORTHCOM.
4. CIP VULNERABILITIES	Identify the top three systemic or across the board vulnerabilities to infrastructure critical to mission accomplishment or other DoD mission essential assets within the organization that receive command awareness at the Service/DoD Agency level (macro-level). Topic areas may be derived from any of the AT Vulnerabilities functional areas. Critical assets may include physical facilities and equipment; computer-based networks; command, control, communication, and intelligence infrastructures; and others as deemed appropriate. **PARAGRAPH INFORMATION REQUIRED:** Identify the vulnerabilities. Provide amplifying discussion on vulnerability, actions taken to mitigate or eliminate the vulnerability, and any lessons learned or TTP's. Identify the type of assistance required (if any) from USNORTHCOM.
5. INSTALLATION CBRNE	Identify the top three systemic or across the board WMD vulnerabilities within the organization that receive command

PREPAREDNESS VULNERABILITIES	awareness at the Service/DoD Agency level (macro-level). Topic areas may range from plans, detection, decontamination, protective systems or capabilities, incident response capabilities or equipment, consequence management capabilities, and others as deemed appropriate. **PARAGRAPH INFORMATION REQUIRED:** Identify the vulnerabilities. Provide amplifying discussion on vulnerability, actions taken to mitigate or eliminate the vulnerability, and any lessons learned or TTP's. Identify the type of assistance required (if any) from USNORTHCOM.
6. HIGH-RISK PERSONNEL (HRP)/HIGH-RISK BILLET (HRB)	Identify Combatant Commander, Service, or DoD Agency designated high risk personnel/billet positions that have qualified personnel and equipment dedicated to performing full-time protective services. *Examples include a Protective Service Detail or Protective Service Operation providing 24/7 coverage during both duty and off-duty time.* **PARAGRAPH INFORMATION REQUIRED:** List name(s) of designated person/rank, duty position, organization, and location.
7. SPECIAL EVENTS/ACTIVITIES	Identify special events or activities that are taking place and where, which may gain national attention or significant media coverage, increases vulnerability, or otherwise presents a large gathering type-target with potential for mass casualties. *Examples include Army-Navy football game; USAFA or MCRD San Diego, CA graduation ceremony; Army 10-Miler; Peterson AFB Air Show; Commissioning of USS Ronald Reagan; etc.* **PARAGRAPH INFORMATION REQUIRED:** Provide information for future events. List name/description of event, location, and date.
8. FP PROGRAM EVENTS	Provide Service/Agency/Activity level significant events, assessments, exercises, conferences, working groups, etc. **PARAGRAPH INFORMATION REQUIRED:** Provide information for future events. Identify the event, date, and provide amplifying details.
9. FP ISSUES OR AREAS OF CONCERN	Identify issues/areas of concern, program information requirements/recommendations, policy issues, etc. for USNORTHCOM consideration/action/situational awareness. **PARAGRAPH INFORMATION REQUIRED:** Identify the issue or topic and provide amplifying details.

Figure R-1

(2) (U) BLUE DART Threat Warning Reports.

(a) (U) Initial Warning Report. BLUE DART warnings will be passed to the threatened unit, activity or location by the most efficient means possible. Initial notification from USNORTHCOM will be passed to the identified service, combatant command, Defense Agency or DoD Field Activity 24-hour/7-day a week operations center or watch and the NMCC. Non-secure communications may be used but only when secure means are unavailable or judged to be too slow. It is inherent upon all DoD Elements to establish written threat warning dissemination procedures to ensure timely introduction of a BLUE DART threat warning to command and control nets, intelligence centers, and across all echelons of the organization.

1. (U) Voice Report Format. BLUE DART threat-warning reports will be passed in accordance with the provided format (Figure R-2).

"This is a real world BLUE DART terrorist threat warning."	(Mandatory Statement)
"This is (Caller's identity) from (Organization) and my unit telephone number is (Telephone number)."	(Mandatory Statement)
"We have information there may be a terrorist attack on (Unit/Activity/Location/Person)."	(Mandatory Statement)
"We believe the attack will take place at (Time/date)."	(Mandatory Statement)
"The attacker will use (type or means) of attack."	(Mandatory Statement)
"(Identity of the attacker) will conduct the attack".	(If known)
"The attack is being conducted because (reason for attack)."	(If known)
"The source of the information is (general description of source's position, access and reliability)."	(If known and only if secure communications are available)

Figure R-2

2. (U) The BLUE DART message receiver will conduct a call back to the message originator/sender to authenticate the identity of the sender and verify the information.

(b) (U) Subsequent (Record Copy) Reports. Initial voice notification to the targeted DoD organization will be followed with FLASH precedence, OPREP-3P record message traffic. This message traffic will be submitted at a minimum to the threatened command/OPCEN, all DOD commands and organizational Headquarters, and the NMCC.

1. (U) BLUE DART message originator utilizes OPREP-3P Message Map IAW CJCSM 3150.03B.

2. (U) Include BLUE DART wording in the message MSGID/OPREP-3P/line of the OPREP-3 message map. Example: MSGID/OPREP-3P/BLUE DART/ unit submitting report/report number//.

3. (U) The following information should be added to GENTEXT/INCIDENT IDENTIFICATION AND DETAILS/ line:

Specific unit/activity/location/persons to be attacked.	(Mandatory)
Specific time and date of attack: DDHHHHZ MM YY	(Mandatory)
Specific type or means of attack.	(Mandatory)
Identity of attackers and reason for attack.	(If known)
Source: Provide original information source, source description, access and assessment of source's reliability or means of learning of the threat.	(If known)
Chronology: Events since reception of information, to include notification of affected unit/activity/location.	(Mandatory)
Originator: POC of reporting organization and time information obtained.	(Mandatory)

Figure R-3

4. (U) OPREP-3P Message Map (Example)

(MESSAGE CLASSIFICATION)
MSGID/OPREP-3P/BLUE DART/USNORTHCOM DWC/ 04-001//
REF/A/USNORTHCOM ASSUMPTION OF CONUS ATFP MISSION/231720ZSEP04//
AMPN/USNORTHCOM EXERCISE OF TACON FOR DOD FORCE PROTECTION AND ASSUMPTION OF OVERALL DOD AT PROGRAM AND FP RESPONSIBILITY IN CONUS//
FLAGWORD/PINNACLE//
TIMELOC/052000ZAUG04/USNORTHCOM/INIT//
GENTEX/INCIDENT IDENTIFICATION AND DETAILS/IMMINENT ATTACK AGAINST FORT HOOD TEXAS EXPECTED AT 061959ZAUG04 BY PERSONNEL USING A VEHICLE BORNE IMPROVISED EXPLOSIVE DEVICE. IDENTITY OF ATTACKERS IS FIVE FOREIGN MALES TRAVELING IN A WHITE VAN AND 24-FOOT LONG RYDER RENTAL TRUCK. ATTACK IS BEING CONDUCTED TO INITIATE A SERIES OF ATTACKS BY THE ARAB BROTHERHOOD BAND (ABB) AGAINST UNIDENTIFIED MILITARY BASES ACROSS THE UNITED STATES. DETAILED SOURCE INFORMATION HAS NOT BEEN DISCLOSED BUT IS DEEMED RELIABLE. INFORMATION IS DEEMED CREDIBLE. MESSAGE RELEASE APPROVAL GRANTED BY THE J3. THIS THREAT INFORMATION WAS OBTAINED THROUGH MULTIPLE SOURCES BY THE USNORTHCOM J2 ON 051400ZAUG04. ADDITIONAL INFORMATION ON THE THREAT CAN BE OBTAINED THROUGH JOHN DOE, USNORTHCOM J2 AT DSN 692-XXXX//
DECL/declassification instructions//

(c) (U) BLUE DART Acknowledgment**.** All DoD Elements are required to ensure that USNORTHCOM receives acknowledgement that the threatened unit/activity/location received the threat warning. Acknowledgement report must be rendered within 30 minutes of notification to the threatened unit and will include DTG message received by the threatened unit, who at the threatened unit/activity/location received the BLUE DART message, and method of receipt or communication (how they were notified). Method of transmission back to USNORTHCOM may be through any appropriate message handling system in OPREP-3 format.

(3) (U) EXERCISE/WHITE PINNACLE/BLUE DART Procedures.

(a) (U) There should never be confusion between actual and exercise BLUE DART messages. An exercise BLUE DART message will never have all three specific criteria areas identified.

(b) (U) Exercise Message Formats. This format will be utilized to initiate a BLUE DART exercise from NCOC and is the format to be used by all exercise participants to disseminate messages. (Figure R-4)

1. (U) Voice Notification.

"This is a BLUE DART exercise. This is not a real-world terrorist threat warning."	(Mandatory Statement)
"This is (Caller's identity) from (Organization) and my unit telephone number is (Telephone number)."	(Mandatory Statement)
"We have information there may be a terrorist attack on (Unit/Activity/Location/Person)."	(Mandatory Statement) (Identify a location; Ft Hood, TX)
"We believe the attack will take place at (Time/date)."	(Mandatory Statement) (Identify a DTG; 061959ZAUG04)
"The attacker will use (type or means) of attack."	(Mandatory Statement) (type or means will be substituted with; EXERCISE EXERCISE)
"(Identity of the attacker) will conduct the attack".	(If known)
"The attack is being conducted because (reason for attack)."	(If known)
"The source of the information is (general description of source's position, access and reliability)."	(If known and only if secure communications are available)

Figure R-4

2. (U) Record Report.

a. (U) BLUE DART message originator utilizes OPREP-3P Message Map IAW CJCSM 3150.03B. Additional guidance for specific lines is provided.

b. (U) Include “WHITE PINNACLE/BLUE DART” wording in the EXER line. Example: EXER/WHITE PINNACLE/BLUE DART//

c. (U) Include “BLUE DART” wording in the message MSGID/OPREP-3P/ line of the OPREP-3 message map. Example: MSGID/OPREP-3P/BLUE DART/ unit submitting report/report number//.

d. (U) The following information should be added to GENTEXT/INCIDENT IDENTIFICATION AND DETAILS/ line. (Figure R-5)

Specific unit/activity/location/persons to be attacked.	(Mandatory)
Specific time and date of attack: DDHHHHZ MM YY	(Mandatory)
Specific type or means of attack.	(Mandatory)
Identity of attackers and reason for attack.	(If known)
Source: Provide original information source, source description, access and assessment of source’s reliability or means of learning of the threat.	(If known)
Chronology: Events since reception of information, to include notification of affected unit/activity/location.	(Mandatory)
Originator: POC of reporting organization and time information obtained.	(Mandatory)

Figure R-5

e. (U) OPREP-3P Exercise Message Map (Example).

(MESSAGE CLASSIFICATION)
EXER/WHITE PINNACLE/BLUE DART//
MSGID/OPREP-3P/BLUE DART/USNORTHCOM DWC/ 04-001//
REF/A/USNORTHCOM CONUS AT OPORD/29JUL04//
AMPN/TAB B TO APPENDIX 1 TO ANNEX C//
FLAGWORD/PINNACLE//
TIMELOC/052000ZAUG04/USNORTHCOM/INIT//
GENTEX/INCIDENT IDENTIFICATION AND DETAILS/IMMINENT ATTACK AGAINST FORT HOOD TEXAS EXPECTED AT 061959ZAUG04 BY PERSONNEL USING EXERCISE EXERCISE. IDENTITY OF ATTACKERS IS FIVE FOREIGN MALES TRAVELING IN A WHITE VAN AND 24-FOOT LONG RYDER RENTAL TRUCK. ATTACK IS BEING CONDUCTED TO INITIATE A SERIES OF ATTACKS BY THE ARAB BROTHERHOOD BAND (ABB) AGAINST UNIDENTIFIED MILITARY BASES ACROSS THE UNITED STATES. ADDITIONAL INFORMATION ON THIS MESSAGE CAN BE OBTAINED THROUGH JOHN DOE, USNORTHCOM J2 AT DSN 692-XXXX//

(4) (U) Vulnerability Assessment (VA) Reporting Requirements.

(a) (U) USNORTHCOM is required to track identified vulnerabilities IAW DoDI 2000.16 (standard 26). Accordingly, all DoD Elements will supply a digital copy of the

final VA report to the Service or Agency Headquarters no later than 60 days after assessment completion. Consistent with DTRA report methodology, all reports will identify vulnerabilities, observations/concerns and observations/positives, and reference them to specific JSIVA alphanumeric benchmarks.

(b) (U) Plan of Action. Within 30 days of receiving a report on a completed assessment, the assessed organization will prioritize, track and report to the next General/Flag Officer the actions to be taken (with suspense established) to address the identified vulnerabilities derived from the assessment. Thereafter, commands will update and report the status of their action plans to the Services/Services designated AT POC on a quarterly basis. A consolidated quarterly Service/Agency report will be forwarded to NC/J34 consisting of assessments completed, assessment results/vulnerabilities, and mitigation plans.

(c) (U) Vulnerability Data Input. Within 30 days of receiving a report on a completed assessment, the Services or designated POC for AT will validate input of vulnerability data has been entered into CVAMP database.

(5) (U) JSIVA/HHQs VA Reporting.

(a) (U) A consolidated quarterly DoD Element report will be forwarded to NC/J34. The quarterly reports will identify annual and triennial program and VAs completed in the quarter, vulnerabilities and mitigation plans (procedural and resource), Risk/Residual Risk Assessment, and identify and highlight recurring deficiencies. The report will state whether the recurrence is either a programmatic or a policy issue.

1. (U) DoD Elements will include interim mitigation measures and level of acceptable risk (relative to FPCON) in the report for programmatic based vulnerabilities.

2. (U) Policy based vulnerabilities will be corrected before the next annual program assessment. DoD Elements will report non-compliance and remedial measures or DoD Element Commander-acceptance of risk to NC/J34.

(6) (U) AT Construction Reporting Requirement.

(a) (U) All existing inhabited structures will be evaluated against the USNORTHCOM construction standards. Each installation/activity commander will submit their plan through their Service headquarters to NC/J34 to evaluate existing inhabited structures (including family housing containing more than 12 units). Each installation/activity will also submit through their higher headquarters, a recurring status report to NC/J34 that delineates the progress made by installation, as well as any steps taken or scheduled, to mitigate the potential of terrorist attack and to prevent mass casualties within existing inhabited structures. Non-DoD owned or controlled facilities will also submit a similar report through their higher headquarters to NC/J34 that delineates the progress made by the organization to integrate into local community/facility emergency response and notification plans as well as any steps

taken or scheduled, to mitigate the potential of terrorist attack and to prevent mass casualties within existing inhabited structures. These reports will be due annually on the 15th of April.

(7) (U) AT Contracting Reporting Requirement.

(a) (U) The DoD Elements will submit annual reports to N-NC/J4C validating that all contracts include DFARS Clause 225.802-70 and all applicable AT clauses in all support contracts. Ensure report contains a list of all support contracts with applicable DFAR and AT clauses.

(b) (U) The DoD Elements that have contracts being performed outside the U.S. and Canada are required to coordinate in advance with the Contract Administration Office (CAO) and obtain required approvals for performance of the contract. In most cases, the CAO will be the local contracting squadron/organization or knowledgeable DCMA Office. Advance communication with the CAO is essential to ensure the installation can provide requested support and to ensure compliance with host/tenant support agreements and Status of Forces Agreements, as applicable. All coordination and approvals should be obtained before solicitation release and must be obtained before award.

(8) (U) Annual AT Exercise Report. Due to USNORTHCOM NLT 15 Oct.

Annual AT Exercise Report			
Percentage of Installations that Conducted an Annual AT Exercise	By-Name List of Those Installations that Have Not Completed an Annual AT Exercise	By-Installation Reasons for Not Completing an Annual AT Exercise	Major Trends/ Lessons Learned (List Top 10)

ANNEX Z TO USNORTHCOM OPORD 05-01 (U)
DISTRIBUTION (U)

DISTRIBUTION C

TAB A TO APPENDIX 3 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
AT EXERCISE PLAN FORMAT (U)

1. (U) Situation

    a. (U) Threat

        (1) (U) Threat Situation
        (2) (U) Threat Level(s) and FPCONs
        (3) (U) USDR Threat Assessment

    b. (U) Friendly

        (1) (U) Own Forces Locations
        (2) (U) Type and Number of Security Personnel and Equipment
        (3) (U) Host Nation security capability

2. (U) FP Mission

3. (U) FP Execution

    a. (U) Commander's Intent (FP)

    b. (U) FP Concept of Operations

        (1) (U) Physical Security at Operation of Exercise Site
        (2) (U) Physical Security at Bed-down Sites
        (3) (U) Transportation Security
        (4) (U) Subsistence Security (food and water protection)
        (5) (U) WMD Preparedness (if required)
        (6) (U) Rules of Engagement (ROE)
        (7) (U) Plan for arming of security personnel
        (8) (U) Movement plan for security personnel/equipment
        (9) (U) Site(s) Layout/Diagram

4. (U) Admin and Logistics

    a. (U) Admin. AT personnel available.

    b. (U) Logistics

        (1) (U) FP Equipment Lists
        (2) (U) FP Maintenance/Storage

5. (U) Command and Signal

a. (U) Signal

(1) (U) Internal Threat Warning Dissemination System
(2) (U) External FP Emergency communications System

b. (U) Command

(1) (U) C2 for FP
(2) (U) DoD Element/Supporting Agency chain of command and responsibilities.
(3) (U) Structure Security Concept Command Relationships.

TAB B TO APPENDIX 4 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
AT PLAN FOR DEPLOYING UNITS (U)

The following sample AT plan is provided as an example only and may be modified to fit the particular mission requirements or situation. The AT plan format in Appendix 4 of DoD O-2000.12H may also be used for deploying units.

1. (U) Purpose. This AT plan promulgates AT policies and procedures of command/unit.

2. (U) Applicability. This AT plan is applicable to: (List all the personnel who must comply with this AT plan.)

a. (U) All assigned and attached (command/unit) personnel.

b. (U) All DoD personnel performing official duties within (location) except (DIA) personnel.

c. (U) All U.S. contractors employed directly by DoD in (location).

3. (U) References.

a. (U) List all applicable references to this AT Plan (i.e., USNORTHCOM AT OPORD).

b. (U) Other references may be applicable to the AT Plan and assist subordinate units determine resources available.

4. (U) Responsibilities

a. (U) The commander is responsible for:

(1) (U) Ensuring implementation of this AT plan for personnel and facilities identified in paragraph 2, above.

(2) (U) Appointing in writing the (____) as AT officer and the (_____) as assistant AT officer, as appropriate.

(3) (U) Appointing high-risk personnel (HRP) security and coordination POCs for each HRP visit, if applicable.

(4) (U) Beginning with this subparagraph, list additional AT oriented specific responsibilities of the commander, as determined by the commander.

b. (U) The (____) security officer is responsible for:

(1) (U) Maintenance of this AT plan per guidance provided in this order.

(2) (U) The conduct and documentation of all training and briefings required by this instruction.

(3) (U) Consolidation of the annual self-inspection/vulnerability assessment and forwarding to higher headquarters as required.

(4) (U) Preparing and submitting requests for armored vehicles if appropriate.

(5) (U) Preparing and submitting the annual armored vehicle report per guidance provided in this order and DoD Directive C4500.51 if appropriate.

(6) (U) Establish a procedure to track open/uncompleted security and safety work requests on facilities (work & domicile).

(7) (U) Beginning with this subparagraph, list additional specific responsibilities of the security officer, as determined by the commander.

c. (U) Individuals identified in paragraph 2, above, are responsible for:

(1) (U) Attendance of AT threat and personal security briefings and documenting their attendance at that training required by the USNORTHCOM AT OPORD

(2) (U) Assist in making family members (14 years of age and over) available to receive AT threat and personal security training as required by the USNORTHCOM AT OPORD.

(3) (U) Accomplishing the annual AT self-inspection and provide the (___) security officer documentation of that self-inspection as prescribed in paragraph 7 of this AT plan.

5. (U) AT Planning

a. (U) Threat Assessments

(1) (U) Threat assessment for this appendix should be classified no higher than Secret. If the threat assessment has a higher classification or the commander’s intent is to keep this document unclassified, insert a reference as to the exact file location.

b. (U) FPCON Supplemental Protective Measures. Commander has supplemented directed FPCON measures identified in Appendix 2.1 with additional measures identified below. The following commander supplemental protective measures will be undertaken and accomplished in addition to directed measures.

(1) (U) FPCON NORMAL. This warrants only a routine posture. No specific measures are identified.

(2) (U) FPCON ALPHA. Beginning with subparagraph (a), Measure 1, list specific FPCON ALPHA protective measures that locally supplement directed protective measures for FPCON ALPHA.

(3) (U) FPCON BRAVO. Beginning with subparagraph (a), list specific FPCON BRAVO protective measures that locally supplement directed protective measures for FPCON.

(4) (U) FPCON CHARLIE. Beginning with subparagraph (a), list specific FPCON CHARLIE protective measures that locally supplement directed protective measures for FPCON CHARLIE.

(5) (U) FPCON DELTA. Beginning with subparagraph (a), list specific FPCON DELTA protective measures that locally supplement directed protective measures for FPCON DELTA.

c. (U) If the AT plan references FPCON measures other than those in this OPORD, a copy of the referenced FPCON measures must be maintained with the AT plan.

d. (U) Suspicious Activity Reporting. List actions to be taken by (command/unit) personnel who identify any type of suspicious activity that may endanger personnel, facilities, or residences (e.g. suspected surveillance, prowler, etc.)

e. (U) Alert Notification Procedures. The Alert Notification System utilized by the command to disseminate AT information, warnings, and/or instructions.

(1) (U) A copy of the Alert Notification System presently in use will be made available to the unit member (identify how a copy of the Alert Notification System may be obtained).

(2) (U) Beginning with this subparagraph, list additional specific information pertaining to Alert Notification Procedures, as appropriate.

f. (U) Maps of Exact Billeting Locations (for medium and high threat areas).

(1) (U) AT or Security officer must identify personnel billeting locations identified in paragraph 2, above. These personnel will provide the Security Officer with a strip-map identifying the exact location of his/her residence within ten working days after arrival in country and/or occupancy of permanent quarters. Billeting strip-maps will be posted and maintained by the security officer or unit as appropriate.

(2) (U) List additional information pertaining to Maps of Exact Billeting Locations of personnel subject to the AT plan.

g. (U) List and Location of Emergency Equipment. Emergency equipment is located as follows:

(1) (U) List location and type of emergency equipment available within the installation; fire equipment, medical equipment, survival food supplies, safe room, etc.

(2) (U) Other Offices/Location: Identify location and type of emergency equipment available.

(3) (U) Billeting (for medium and high threat areas): List the type(s) of emergency equipment available within personnel billeting, such as fire escape equipment, extinguishers, smoke detectors, 2-way radios, telephones etc.

(4) (U) Evacuation and Assembly Points: List unclassified location(s) and type of emergency equipment available at evacuation and assembly points. If evacuation and assembly locations are classified, identify it as such, and use this subparagraph to inform personnel exactly where they may find the information.

h. (U) Public Affairs Responsibilities. Discuss the responsible agent(s) for release of information regarding AT planning or terrorist incidents.

i. (U) Health Services. Plan for medical support to include first aid and transport of casualties from point of injury/illness to a medical facility. Plan should contain procedures to contact response/transportation agencies to be used in emergencies.

6. (U) AT Briefings.

a. (U) New Arrival AT Threat and Personal Security Briefings.

(1) (U) All new arrivals identified in paragraph 2, above, will be given an AT threat and personal security briefing within 72 hours of their arrival in an area at FPCON BRAVO or higher. A significant part of the military member’s introduction should be a review and familiarization of this AT Plan. NOTE: Present AT information in a balanced manner. Exaggeration could cause undue anxiety but a lack of correct emphasis could also contribute to poor AT practices.

(2) (U) Following the new-arrival AT threat and personal security briefing and review of this AT plan, an attendance roster or individual training/briefing letter will be annotated.

b. (U) Annual AT Threat and Personal Security Briefing.

(1) (U) All personnel identified in paragraph 6a above will attend, as a minimum, annual (refresher) AT threat and personal security briefing. Although required annually, refresher briefings may be conducted more frequently if required. For personnel

assigned to Significant or higher threat areas this training will include guidance on appropriate conduct in the event they are taken hostage or kidnapped.

(2) (U) Following accomplishment of the annual (or refresher) AT Threat and Personal Security Briefing, individuals will sign an attendance roster or an individual training/briefing letter will be annotated.

7. (U) AT Self-Inspections and Physical Security Vulnerability Assessments.

a. (U) Each unit/individual as applicable identified in paragraph 2 above should complete an AT self-inspection and a physical security vulnerability assessment on an annual basis (determine an appropriate timetable or due date).

b. (U) Provide the completed self-inspection(s) and vulnerability assessment(s) to the AT officer who will evaluate the results and forward deficiencies as required.

c. (U) In addition to the completed self-inspections/vulnerability assessments, units/personnel completing self-inspections/vulnerability assessments will provide the security officer any work orders to correct physical security deficiencies they may have noted during their inspection.

d. (U) Completed self-inspections will be maintained on file as for a minimum of two years.

8. (U) Armored Vehicles.

a. (U) Fully Armored Vehicles (FAV). Specific information or guidance pertaining to FAVs, as appropriate.

b. (U) Light Armored Vehicles (LAV). Specific information or guidance pertaining to LAVs, as appropriate.

c. (U) Other Vehicle Information. Specific information or guidance pertaining to vehicles, as appropriate. Concerns such as exhaust pipe modifications to prevent the insertion of explosive devices, AT physical security practices and operational security practices should be addressed.

9. (U) High Risk Personnel (HRP).

a. (U) List additional specific information or guidance pertaining to HRP, as appropriate.

b. (U) Actions to be taken in preparation of HRP visit:

(1) (U) The commander is responsible for coordinating and arranging security for HRP visitors.

(2) (U) The commander will designate a security POC for each HRP visit and required coordination.

(3) (U) Designated HRP POC will advise and coordinate visit security requirements with the command/unit as appropriate.

10. (U) Control of Information Relating to HRP.

a. (U) Classification of HRP itineraries.

b. (U) Unclassified schedules or portions of HRP itineraries.

c. (U) Public release of information pertaining to HRP visit.

11. (U) Billeting Security.

a. (U) The security officer will ensure personnel assigned in an area evaluated as either a medium or higher threat, are either provided with on-installation or other government quarters or are provided specific guidance on AT factors to consider in selecting private residences. They will also ensure a physical security assessment of off-installation residences of permanently assigned/TDY/TAD personnel and, based on the results of this assessment, provide AT recommendations to these residents. For combatant forces, installation Commanders will establish minimum-security standards.

b. (U) The security officer will maintain copies of all residential security related work orders submitted for corrective action.

c. (U) Work order records maintained in this AT plan will be utilized to ensure residential security upgrades are accomplished and for future reference, as well as to aid in fiscal planning.

d. (U) Beginning with this subparagraph, list any additional (SAO)-specific information or guidance pertaining to residential security, as appropriate.

12. (U) Additional subparagraphs should be considered to further expand this plan.

a. (U) AT plans for deploying units and elements will include response procedures to terrorist incidents to include but not be limited to the threat of WMD, medical response and management capabilities, off-post personnel notification and recall procedures, security forces response, and an attack warning system with recognizable alarms and actions for potential emergencies. The warning system must be exercised to ensure personnel are trained and proficient in recognition of an impending attack. Ensure all aspects of and assumptions in the AT plan that can be are exercised and validated prior to deployment, recognizing that some aspects of the deployment AT plan

cannot be exercised until arrival at the deployed location. The unit commander as soon as feasible will exercise the following AT plan execution items:

1) (U) Immediate incident response and post-incident actions.

(2) (U) Effectiveness of command and control systems.

(3) (U) Terrorist Incident Crisis Management. Ensure a common baseline Deviations or waivers must be coordinated and approved by message with NC/J34.

(4) (U) All personnel receive pre-deployment AT awareness training.

(5) (U) Ensure all deploying personnel are briefed on the local threat.

(6) (U) All personnel performing law enforcement, security or homeland defense duties in the AOR will be knowledgeable of the USNORTHCOM Arming, and Use of Force Policy and, if appropriate, specific Rules of Engagement for the situation. These policies will apply to all forces assigned to USNORTHCOM.

(7) (U) Ensure a tailored, site-specific physical security system is developed and deployed for all installations and in-transit stops. The components of this physical security system must be included in the AT Plan.

(8) (U) Ensure all personnel are medically cleared (physically and psychologically), have the proper immunizations and receive a briefing from medical personnel on health issues at the deployed location.

(9) (U) Maintain a current copy of this OPORD and appoint in writing a CBRNE Defense Officer primary and alternate to develop, implement, and supervise the unit's CBRNE Defense Program in accordance with the provisions of this OPORD.

(10) (U) Units will develop a CBRNE Defense Plan and include this plan as an annex to the AT plan.

13. (U) Personnel authorized Individual Protection Equipment, to include contractors that are supporting contingency operations or units deploying for more than 15 days to the locations within USNORTHCOM where a CBRNE threat is present will be assigned CBRNE Individual Protection Equipment consistent with service specific requirements.

14. (U) Submit an after-action report (AAR) to their DoD Element or joint force headquarters, with a copy to NC/J34, within 30 days of completing the deployment (applies to OCONUS in USNORTHCOM AOR only; CONUS when in support of USNORTHCOM; and as required by the Commander, USNORTHCOM based on the threat). This AAR should be classified as appropriate and, as a minimum, include the following areas:

a. (U) An overview to include unit name, dates, locations, FPCON, threat levels, and brief description of friendly forces, to include the host location.

b. (U) Comments on U.S. friendly forces support.

c. (U) Comments on medical care received from other than U.S. forces, to include other friendly forces.

d. (U) Any AT observations relevant to the visit. Comments should include: traffic flow, type of service vehicles encountered, the methods used to screen such vehicles, convoy operations, billeting and security measures taken.

e. (U) Describe problems encountered in implementing or conducting AT measures. Specifically, address means employed to establish perimeters and whether it effectively controlled unauthorized pedestrian or vehicle traffic, means of inspecting and /or authorizing service vehicles, C2, and response options for unauthorized approaches.

f. (U) Comment on any helpful POCs, along with contact numbers and support provided.

g. (U) Contact respective Unified Command CISO regarding any contact with foreign government personnel or foreign nationals who make suspicious requests for information about self, duties or organization. Report any unsolicited/unauthorized requests for information and report any suspected surveillance by host nation or foreign nationals, or foreign intelligence services.

ANNEX A: AT PLAN REFERENCES (U)
TAB 1 – USNORTHCOM AT OPORD (U)
TAB 2 – DoD Directive 2000.12, DoD Antiterrorism Program (U)
TAB 3 – DoD Instruction 2000.16, DoD Antiterrorism Standards (U)
TAB 4 – DoD Handbook O-2000.12-H, DoD Antiterrorism Handbook (U)
TAB 5 – DoD Directive C-4500.51, DoD Non-Tactical Armored Vehicle Policy (U)
TAB 6 – U.S. Embassy, (country), Emergency Action Plan (EAP) (U)
TAB 7 – Beginning with this Tab, insert other references that complement the AT Plan (U)

ANNEX B: AT PLAN THREAT ASSESSMENTS (U)
TAB 1 – USNORTHCOM-provided threat assessment for (country) (U)
TAB 2 – DIA-provided threat assessment for (country) (U)

ANNEX C: ALERT NOTIFICATION PROCEDURES (U)
Include in this annex a copy of the Alert Notification Procedures. Ensure all personnel/units subject to the AT plan are identified in notification procedures.

ANNEX D: MAPS OF EXACT BILLETING LOCATIONS (U)
Include in this annex maps of exact residential locations of all personnel subject to the AT plan, if applicable. If not located here, identify location of residential maps (i.e., unit orderly room).

ANNEX F: ASSESSMENTS (U)
TAB 1 - Higher headquarters vulnerability assessments/self-inspections. (U)
TAB 2 - Consolidated unit self-inspections. (U)
ANNEX G: RESIDENTIAL SECURITY WORK ORDERS (U)
Include copies of security work orders.

TAB C TO APPENDIX 4 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
UNITED STATES DEFENSE REPRESENTATIVE (USDR)/UNITED STATES DEFENSE ATTACHÉ OFFICER (USDAO) COUNTRY POINTS OF CONTACT (U)

The following personnel are the USDR/USDAO POCs for the listed country.

a. (U) Puerto Rico: (a commonwealth of the US) and U.S. Virgin Islands (unincorporated territory of the US) both fall under U.S. sovereignty and, therefore, there are no Military Liaison Officers or Defense Attaché Offices (DAO) for these areas.

b. (U) Caribbean Island Nations: Cuba and the Bahamas have liaison officers but the Unified Command Plan assigns security cooperation for those nations to USSOUTHCOM. The Turks, Caicos, and British Virgin Islands fall under USNORTHCOM for security cooperation.

Country	City	Address	Phone	Ambassador	DAO
Canada	Ottawa, Ontario	490 Sussex Drive Ottawa, Ontario Canada KIN 1G8	(613) 238-5335	Paul Cellucci	Col David Brackett (613) 688-5400
Mexico	Mexico City	Paseo de la Reforma 305 Col. Cuauhtemoc 06500 Mexico	[52](55) 5080-2000	Antonio Garza	COL Leocadio Muniz [52](55) 5080-2000, x4109
Cuba	Havana	Swiss Embassy Calzada between L and M Streets Vedado, Havana	[53](7) 833-3551/9	James Cason	Liaison (no DAO): Ronald Pailliotet 011-537-833-3551
Bermuda	Hamilton (CG)	Crown Hill 16 Middle Road Devonshire	[441] 295-1342	(CG) Vacant Antoinette Boecker	For London & Bermuda (Residence in London) CAPT David L. Wirt, USN 44 (0) 207894-0745
Turks & Caicos					
British Virgin Islands					

TAB A TO APPENDIX 5 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
TRAVELER FPCON PROCEDURES (U)

(U) General Information: Traveler FPCON measures are not blanket applications. These are directed as needed and are applied when the threat level dictates regardless of CONUS or OCONUS application. All personnel traveling on temporary duty (TDY/TAD) or leisure travel to or through USNORTHCOM AOR areas designated Significant or High Threat Levels will receive appropriate threat briefings. These FPCON measures apply to individual travelers and to small groups of travelers that are required to travel during heightened periods of alert. Personnel from other Combatant Commands and those personnel traveling OCONUS within the USNORTHCOM AOR are required to complete Level I training before official travel to the USNORTHCOM AOR.

1. (U) FPCON Normal. Local security measures designed for implementation when there is no credible threat of terrorist activity.

2. (U) FPCON ALPHA Measures.

a. (U) Traveler ALPHA 1. Obtain and follow measures the local commander implements to increase security. Review AT awareness procedures.

b. (U) Traveler ALPHA 2. Maintain regular contact with the nearest military installation, U.S. security agency/element, and/or local security elements, as well as the home station.

c. (U) Traveler ALPHA 3. Review your emergency action plan. Ensure all personnel in your party are familiar with the plan.

d. (U) Traveler ALPHA 4. Confirm/Identify protected and/or safe areas you can rapidly move to before or during an incident.

e. (U) Traveler ALPHA 5. Increase liaison with any available security agency (hotel, residential, etc.). Notify security agencies if security measures could affect their operations.

3. (U) FPCON BRAVO Measures.

a. (U) Traveler BRAVO 1. Cease wearing U.S. military uniforms in non-secure areas.

b. (U) Traveler BRAVO 2. Do not travel with easily identifiable military luggage (i.e. duffel bags, B-4 bags) or military tags or organizational identification.

c. (U) Traveler BRAVO 3. If practical, follow the “buddy rule” for all movement.

d. (U) Traveler BRAVO 4. Periodically exercise AT contingency plans and drills.

e. (U) Traveler BRAVO 5. Routinely check your vehicle(s) for improvised explosive devices (IEDs) or tampering.

f. (U) Traveler BRAVO 6. If practical, park your vehicle(s) in secure areas, not accessible to uncontrolled personnel.

g. (U) Traveler BRAVO 7. Vary routines.

h. (U) Traveler BRAVO 8. Conduct weekly telephone liaison with nearest military installation, nearest U.S. security agency/element, and/or local security elements and home station.

i. (U) Traveler BRAVO 9. Determine and avoid high-risk areas and be cautious of mingling with crowds.

4. (U) FPCON CHARLIE Measures.

a. (U) Traveler CHARLIE 1. Determine the nature of the imminent threat; members should contact the nearest U.S. military installation or embassy/consulate for additional information or instructions if there is any change in the local U.S. Threat Advisory as published by the Department of Homeland Security or Department of State/Host Nation Threat Advisories for OCONUS locations.

b. (U) Traveler CHARLIE 2. Individuals will not travel into an area at FPCON CHARLIE or above unless the mission is deemed essential. If an area is placed at FPCON CHARLIE, contact your commands to determine if they are considering withdrawing you or your party.

c. (U) Traveler CHARLIE 3. Security personnel, trained in terrorism counteraction, will accompany large or high-risk groups traveling to an area at FPCON CHARLIE. The Supporting Service Commander/subordinate/joint force commander will determine the risk.

d. (U) Traveler CHARLIE 4. Travelers will review all personal emergency contingency and emergency planning, exercising applicable measures as necessary. Ensure family members and co-travelers are aware of the situation and contingency plans as necessary and appropriate.

e. (U) Traveler CHARLIE 5. Conduct daily telephone liaison with nearest U.S. Military installation, nearest U.S. security agency/element, and/or local security elements and home station.

f. (U) Traveler CHARLIE 6. Treat all mail packages as a potential IED. Conduct limited inspections for explosive or incendiary devices, or other dangerous items.

g. (U) Traveler CHARLIE 7. Cancel all official social events outside of a secured facility or installation. Severely limit social activities. Do not visit high-risk areas.

h. (U) Traveler CHARLIE 8. Team Leaders of small deployments will consider canceling leave or passes as appropriate to the circumstance and contact their commanders to determine if the mission should be cancelled. Leisure travelers will contact their respective command authorities to determine if the commander is canceling leave and/or passes as appropriate to the circumstances.

i. (U) Traveler CHARLIE 9. Travelers traveling to and from the installation to off-base locations will not wear visible uniforms when traveling off base.

5. (U) FPCON DELTA Measures.

a. (U) Traveler DELTA 1. Move to a protected area.

b. (U) Traveler DELTA 2. Treat all unidentified vehicles and containers as a potential IED.

c. (U) Traveler DELTA 3. Minimize, cancel or delay all non-essential movement.

d. (U) Traveler DELTA 4. Conduct routine liaison checks as established with the nearest U.S. military installation, nearest U.S. security agency/element, and/or local security elements and home station.

e. (U) Traveler DELTA 5. Cancel all social activities.

TAB B TO APPENDIX 5 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
DEPLOYED UNIT FPCON PROCEDURES (U)

1. (U) Deployed unit FPCON procedures are not blanket applications. These are directed as needed and are applied when the threat level dictates regardless of CONUS or OCONUS application. When appropriate, coordinate these measures with the local law enforcement agencies or the COM for OCONUS deployments in accordance with existing CONPLANs/OPLANs when operating in support of USNORTHCOM.

2. (U) FPCON NORMAL. Local security measures designed for implementation when there is no credible threat of terrorist activity.

3. (U) FPCON ALPHA.

a. (U) Deployed Unit ALPHA 1. Brief all deployed personnel on the current threat condition and reason for implementation of higher FPCON. Review those antiterrorism measures enacted to increase security.

b. (U) Deployed Unit ALPHA 2. Review unit-level terrorism awareness training.

c. (U) Deployed Unit ALPHA 3. Test radio and telephone communications monthly.

d. (U) Deployed Unit ALPHA 4. Increase liaison with local agencies via established chains of command to assist in monitoring potential threats.

e. (U) Deployed Unit ALPHA 5. As a deterrent, randomly use trained explosive ordnance detection dog (EODD) teams, if available.

f. (U) Deployed Unit ALPHA 6. Advise all personnel of, and to avoid, high-risk areas and be cautious when mingling with crowds.

4. (U) FPCON BRAVO.

a. (U) Deployed Unit BRAVO 1. Establish an operations watch/center to handle force protection, including handling security posts, reaction forces and responses to attack.

b. (U) Deployed Unit BRAVO 2. Ensure all guard posts are manned by at least two personnel armed with individual weapon and basic load.

c. (U) Deployed Unit BRAVO 3. Provide for an armed reaction force

d. (U) Deployed Unit BRAVO 4. Reserved for future use.

e. (U) Deployed Unit BRAVO 5. Brief command representatives of all units and activities at the deployment site concerning the threat and security measures implemented in response to the threat. Implement procedures to provide periodic updates for these unit and activity representatives.

f. (U) Deployed Unit BRAVO 6. Periodically exercise antiterrorism contingency plans and drills.

g. (U) Deployed Unit BRAVO 7. Test radio and telephone communications weekly.

h. (U) Deployed Unit BRAVO 8. Conduct identity checks of all personnel entering secure areas and other sensitive activities. Increase the frequency of random identity checks of personnel at the deployment site.

i. (U) Deployed Unit BRAVO 9. Establish concentric zones of security. Assign sectors of responsibility to units to defend during an attack.

j. (U) Deployed Unit BRAVO 10. Ensure personnel traveling away from the deployment site leave at least one individual to protect and secure vehicles in unsecured areas. Implement a convoy security plan for all vehicles leaving the deployment site.

k. (U) Deployed Unit BRAVO 11. Implement the buddy rule for all personnel departing the deployment location. Review unit liberty policy and revise it as necessary to enhance force protection.

l. (U) Deployed Unit BRAVO 12. Implement the buddy rule for all personnel on liberty.

5. (U) FPCON CHARLIE.

a. (U) Deployed Unit CHARLIE 1. Units will not deploy/travel into an area at FPCON CHARLIE or above unless the mission is deemed essential.

b. (U) Deployed Unit CHARLIE 2. Units deploying to an area at FPCON CHARLIE will deploy with military police or other elements trained in terrorism counteraction.

c. (U) Deployed Unit CHARLIE 3. Implement a two-vehicle rule for all vehicles exiting secured areas.

d. (U) Deployed Unit CHARLIE 4. Put reaction force on 15-minute standby.

e. (U) Deployed Unit CHARLIE 5. Provide ammunition for all armed personnel. Load weapons at the commander’s discretion.

f. (U) Deployed Unit CHARLIE 6. Request host nation law enforcement/ security forces to augment/reinforce security forces.

g. (U) Deployed Unit CHARLIE 7. Request local law enforcement provide additional security for vehicles traveling away from the deployment site.

h. (U) Deployed Unit CHARLIE 8. Conduct identity checks of all personnel entering the deployment site. Conduct detailed vehicle inspections (trunk, undercarriage, glove boxes, etc.) of all vehicles and interior inspections of all containers and packages.

i. (U) Deployed Unit CHARLIE 9. Implement centralized parking for all vehicles. Park vehicles at least 110 meters away from sensitive areas. Implement a shuttle service if required.

j. (U) Deployed Unit CHARLIE 10. If available, employ antiterrorism security devices, including ground surveillance radar, bomb detection devices, thermal imaging systems, etc.

k. (U) Deployed Unit CHARLIE 11. Based on the threat, construct blast/defensive bunkers/positions to protect personnel in threatened areas.

l. (U) Deployed Unit CHARLIE 12. Cancel all official social events. Advise all personnel to severely limit social activities. Place all high-risk areas off limits.

m. (U) Deployed Unit CHARLIE 13. Cancel unit liberty.

6. (U) FPCON DELTA.

a. (U) Deployed Unit DELTA 1. Move personnel to blast/defensive bunkers.

b. (U) Deployed Unit DELTA 2. As feasible, arm all available personnel.

c. (U) Deployed Unit DELTA 3. Augment guard forces to ensure positive control and sectors of fire over the entire deployment site.

d. (U) Deployed Unit DELTA 4. Frequently inspect outlying areas or exteriors of facilities and parking areas.

TAB B TO APPENDIX 6 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
SECURITY ASSESSMENT CHECKLISTS (U)

SECURITY ASSESSMENT/SURVEY CHECKLISTS

1. (U) The following three checklists are included to provide users of this OPORD a resource with which to conduct detailed security assessments of installation/activity/facility vulnerabilities. These checklists are designed as guides, which users may and should modify for their own use.

a. (U) The first checklist (General Physical Security) is designed to assist in conducting security assessments of installations and facilities, and focuses on the collection of detailed physical security data to support security assessments using the checklist in Tab C of this Appendix:

(1) (U) Where the threat and/or the number of DoD-assigned personnel do not meet HHQ VA thresholds.

(2) (U) To assess the vulnerability of non-DoD facilities (ports and airfields) used infrequently by DoD personnel.

b. (U) The Survey Checklist For Residential Security and Personal Security Practices is designed to assist in evaluating off-installation and on-installation residences as well as the personal security practices of individuals and family members.

c. (U) The Security Survey Worksheet for High-Rise Commercial Buildings, is offered to assist in the evaluation of work areas, primarily off an installation, but it also may be useful when looking at commercial hotels as potential troop billeting facilities

2. (U) DoD Handbook O-2000.12-H provides additional checklists for various other types of facilities.

FOR OFFICIAL USE ONLY

General Physical Security CHECKLIST

A. GENERAL			
1. Individual (s) conducting survey:			
Name:			
Rank/Grade:			
Organization:			
Phone Number:			
2. Survey Date(s):			
3. Description of facility surveyed:			
4. Individual (s) interviewed:			
	Interviewee 1	Interviewee 2	Interviewee 3
Name			
Rank/Grade			
Organization			
Phone Number			
5. Obtain plot plan of the entire facility area showing:			
(a) Compass rose showing north			
(b) All existing buildings and their function, all interior and exterior roads, all fences, and other physical barriers			
(c) Railroad sidings or main track			
(d) Airfield facilities including runways, taxiways, helipads, supporting utilities, or utilities lying beneath such surfaces			
(e) Location of gates (active and inactive)			
(f) Parking lots/areas, and types of personnel using them			
(g) Any planned remodeling or expansion of facilities.			
6. Obtain as-built drawing of the office or residential structure showing:			
(a) Construction of exterior and interior walls			
(b) Location of all windows, doors, and skylights			
(c) Location and size of all vents, utility openings, other building penetrations			
(d) Electrical runs, outlets, and switches for all voltages.			
7. Location of facility (check as applicable and describe)			
oUrban			
oSuburban			
oIncorporated			
oUnincorporated			
oGovernment Installation			

8. Socioeconomic environment (check one, describe)			
oResidential			
oIndustrial			
oCommercial			
oAgricultural			
(a) Neighboring area is: o Affluent o Middle Class o Poor			
(b) Comments:			
9. Area crime rate: o High o Moderate o Low			
(a) Is the area in a high crime environment:			
(b) Neighborhood violence:			
(1) Civil unrest			
(2) Robberies			
(3) Burglaries			
(4) Assaults			
(5) Homicides			
(6) Narcotics trafficking			
(c) Is there a history of loss at this facility:			
(d) Types of losses			
(1) Number of Pilferage	Value	Dates	
(2) Internal theft	Value	Dates	
(3) Burglary/B&E	Value	Dates	
(4) Vandalism	Value	Dates	
(5) Property Losses	Value	Dates	
Comments			
10. Law enforcement agency (host nation if applicable) having jurisdiction:			
Name			
Chief/Supervisor			
Location			
Phone Number			
Average response time			
11. Is liaison maintained with host nation law enforcement agencies? oYes o No			
12. Is there an active security awareness program? o Yes o No			
13. Number of employees			
14. Are background investigations conducted before employment of any personnel?			
15. What categories of personnel are investigated?			
16. What is the extent of the investigation? Conducted by whom?			
17. Number of personnel requiring entrance and exit to structure/facility/site/installation:			
0700-0800:	1000-1100:	1300-1400:	1600-1700:
0800-0900:	1100-1200:	1400-1500:	1700-1800:
0900-1000:	1200-1300:	1500-1600:	1800-1900:
18. Comments regarding access:			

B. PERIMETER SECURITY
1. Physical barriers:
(a) Is there some type of physical barrier around this facility?
Describe
(1) Does the barrier establish the property line?
(2) Is it a deterrent to entry?
(3) Does it establish personnel control?
(4) Does it establish vehicle control?
(5) If any holes exist in the fence, where are they located?
(6) Are there any places along the fence where the ground is washed away?
(7) Are there any places where streams circumvent the fence?
(8) How are these areas protected?
(9) Is there an adequate clear zone existing on both sides of the fence?
(10) Is the clear zone obstructed by material being stored near the fence?
(11) Are there any poles near the fence where they can be used for entry or exit?
(12) Are there any trees in the clear zone?
(13) Are the trees acceptable, or should they be removed or trimmed?
(14) Is there any shrubbery, underbrush, or high grass in the clear zone?
(15) Is there any scheduled action taken to remove or keep growth in the clear zone cut so that it does not obstruct a clear view of the fence?
(16) Are there any openings other than gates and doors in the fence that are not protected?
(17) If protected, is it adequate?
(18) Are there NO TRESPASSING signs posed on the outside of the fence at regular intervals? Are they printed in common local languages as well as in English?
(19) Is the entire fence line within easy view of patrolling guards or CCTV?
(20) Is the entire fence line in view of assigned personnel during normal working hours?
(21) Is the fence inspected?
(22) If so, how often and by whom?
(23) Is immediate action taken to repair reported fence damage?
(24) Are vehicles allowed to park near perimeter physical barrier?
(25) Is material stacked near perimeter physical barrier that would act as a stepladder or otherwise assist either penetration or egress through the barrier?
2. Gates and Doors
(a) How many gates are there through the perimeter?
(b) How many doors are there through the perimeter?
(c) List all doors and gates, designating the use of each including those not used at all. This would include doors and gates through the perimeter used for employees (if separate categories of employees use different doors or gates, designate the category for each), those use for visitors, private vehicles, delivery and shipment trucks, railroad

sidings, those rarely used, and those not used at all. Each gate should be identified by number or name, the hours used, and how each is controlled.
(d) How are these gates monitored?
(f) Are all gates adequate secured and operating properly?
(g) Do swing gates close without leaving a gap?
(h) Are gates that are not used or only rarely used equipped with proper locks and seals?
(i) Are chains and locks of adequate construction used to secure gates when closed and locked?
(j) Are alarm devices used on any gates?
(k) Are exit alarms used on perimeter fire doors or other doors that are not available for general use?
(l) Are exit alarms used? Do they provide a local signal, a signal at a guard office, or both?
(m) Are there any doors or gates through the perimeter where CCTV could be used to control admittance and exist?
(n) How many persons would use doors and gates at peak periods?
(o) Would these doors or gates have to be available for use at odd hours?
(p) Are there any gates or doors where CCTV could be used for ingress and egress of vehicles and trains?
(q) What are the peak periods of traffic through these gates?
(r) Are these gates or doors used regularly during operating periods?
(s) Are these gates or doors used normally during closed periods?
(t) How often are these gates generally used during open and closed periods?
(u) What is the normal number of vehicles/railroad cars that would pass through these gates or doors during a 24-hour period?
(v) Could any of the personnel doors of the type described above be adequately secured by permitting entry and exit with a card-key operated turnstile-type gate without the use of CCTV?
(w) Are gates and doors through the perimeter posted with NO TRESPASSING signs in English and other locally used languages?
(x) Are any of the entrances-exits through the perimeter presently controlled by CCTV and/or card-key locks and turnstiles?
(y) Can vehicles drive up to the fence and be used as a stepladder for entry or exist?
(z) Is there a railroad gate?
(1) Does the railroad have a lock on the gate?
(2) Does the DoD activity have a lock on the gate?
(aa) Comments:
C. PERIMETER LOCK SYSTEM
1. Locks
(a) What type of locks are used?
(b) Name of manufacturer
(c) Are cylinders removable? o Yes o No

(d) Are locks changed when security may be compromised? o Yes o No	
(e) When were locks last changed?	
(f) When were locks last inspected?	
(g) What is the condition of the locks?	
(h) Are locks adequate?	
(1) Case hardened padlocks? o Yes o No	
(2) Case hardened chains? o Yes o No	
(i) Are all lock numbers recorded? o Yes o No	
(j) Are numbers obliterated? o Yes o No	
2. Key control	
(a) Who is responsible for key control?	
(b) Are keys signed for?	
(c) Are door locks and padlocks separate systems?	
3. Comments	
D. PERIMETER ALARM SYSTEMS	
1. Perimeter alarms	
(a) Are perimeter alarms employed? o Yes o No	
(1) Manufacturer	
(2) Is the alarm: Local o Yes o No	
Central Station o Yes o No	
Silent o Yes o No	
Direct (Police) o Yes o No	
(3) Installation Date	
(4) How many points alarmed?	
(i) Location of each alarm contact	
(ii) Location of master control box	
2. Inspection and maintenance	
(a) Date of last inspection	By whom?
(b) Date of last service	By whom?
(c) Is there a maintenance contract?	Cost
3. What are the local laws regarding false alarms?	
4. What is normal response time to an alarm?	
5. Alarm system details	
(a) Are wires going to local alarm protected, i.e. in conduit? o Yes o No	
(b) If a perimeter alarm detector is used, does restoring door or window to original position stop alarm? o Yes o No	
(c) Does alarm have a battery back-up o Yes o No	
(d) Is battery checked periodically for suitable charge o Yes o No	
(e) Are duress alarms used at any point? o Yes o No	
6. Comments	

E. PERIMETER LIGHTING	
1. Are all perimeter areas lighted during hours of darkness o Yes o No	
Explain (If answer is no)	
2. What type of lighting is used?	
3. Is lighting manual or automatic?	
4. Are all entrance and exit gates well lighted? o Yes o No	
Exceptions	
5. Does perimeter lighting also cover the buildings? o Yes o No	
6. If lights burn out, do light patterns overlap? o Yes o No	
7. Is someone responsible for turning lights on and off? o Yes o No	
(a) If so, whom?	
(b) Who is responsible for lighting maintenance?	
(c) Are there adequate supplies on hand for maintenance of lighting system (bulbs, fuses, etc.) o Yes o No	
8. Are guards exposed or protected by the lighting?	
9. Are gates adequately lighted?	
10. Do lights at gate illuminate interior of vehicles?	
11. Are critical and vulnerable areas well illuminated?	
12. Are perimeter lights wired in series or parallel?	
13. Is there an auxiliary power source available?	
(a) Automatic or manual start?	
(b) Who is responsible for manual start?	
14. Comments	
F. GUARD SERVICE	
1. Is a guard service employed? o Yes o No	
oContractor o U.S. Military	
oForeign Military o Foreign Police	
2. Contractor name and address:	
(a) Contractor representative	
(b) Telephone number	
3. Have written instructions been issued to the guards as to their duties and assignments? o Yes o No	
4. Are guards free from "extra duties" so they are able to perform their protective duties? o Yes o No	
If not, explain:	
5. Days per week guards secure facility	
6. Guard force hours:	
(a) Day Shift	Number of Guards
(b) Evening Shift	Number of Guards
(c) Night	Number of Guards
7. Current rate paid for guard service	

(a) Hourly wage rate for guards	
(b) Is there a contract in effect	
8. Are clock stations used?	If so, how many
(a) Are all clock charts reviewed daily?	
(b) Who reviews them?	
9. Are activity reports prepared by guards for each shift?	
(a) Irregularity reports	
(b) Who reviews reports?	
10. Do guards have keys to gates?	Buildings?
(a) How are the keys controlled?	
11. Are guards armed?	
(a) Have they received weapons instruction?	
(b) If so, how often?	
(c) By whom?	
12. Do the guards take periodic polygraph examinations? o Yes o No	
(a) How often?	
(b) Who gives them?	
13. What type of communication system is used? (Primary "P", Backup "B")	
Telephone	
Radio	
Pak sets	
Alarm switch	
14. Comments	
G. INTERIOR	
(Note: use a separate sheet for each office, building, or residence.)	
1. Description of building Purpose of building	
2. Doors or openings	
(a) How are doors constructed: o Wood o Metal	
(b) Describe types of security locks used: (Manufacturer/type)	
(c) Are hinges and lock hasps securely installed?	
(d) How are doors locked or barred during non-working hours?	
(e) Who is responsible for making sure doors are secured?	
(f) Are all windows that are not used, permanently closed?	
(g) Are all accessible windows protected by heavy wire mesh or bars?	
(h) If windows are covered by wire mesh, are the mesh coverings fastened from the inside or secured with locks?	
(i) Describe window frames in terms of materials used and type of construction.	
(j) Have windowpanes been hardened? How?	
(k) If windows can be opened and are locked, are they protected by ordinary window lever locks or key locks?	

(l) Is the general security of windows facing on the perimeter adequate?		
(m) Are all accessible skylights, doors, and other openings adequately secured?		
(n) Are there any ladders (permanent or temporary) that should be removed, secured, or blocked from unauthorized used?		
H. OBSCURE OPENINGS		
1. Are there any sidewalk elevators at this facility?		
If so, are they properly secured when not in operation?		
2. Are sidewalk elevators secured during operation?		
3. Do storm sewers or utility tunnels breach the outer barrier?		
4. Are these sewers or tunnels adequately secured?		
5. Are there any openings from these utility tunnels or storm sewers, i.e., manholes, inside the facility?		
(a) Are all power facilities, transformers, and other critical utilities equipment adequately protected? Explain:		
I. OFFICE OPERATIONS/ACCESS CONTROL		
1. What are normal working hours?		
HOURS	NO. OF PERSONNEL	NO. OF SUPERVISORS
2. Days per week of operation		
3. Employee identification		
(a) Is employee ingress/egress restricted to controlled entrances and exits?		
(1) Controlled by:		
o Badge		
o Pass		
o Guard		
o Key		
o Receptionist		
(b) Do all employees have badges?		
(c) Do employees wear ID badges with pictures on them? o Yes o No		
(d) Is the egress/ingress control point used for employees the same as the one used for visitors, vendors, repairmen, etc.? o Yes o No		
4. Who opens in the morning?		
5. Who closes in the evening?		
6. Comments		
J. PARKING		
1. Parking area(s)		
(a) Approximate size		
(b) Inside fence		
(c) Outside fence		
(d) Distance nearest vehicle to fence		
2. Number of automobiles parked daily		

3. Are places assigned?
(a) Location of visitor parking
(b) Lighting
(c) Patrolled by guards
(d) Observed by CCTV
(e) Are parking permits or decals used?
4. Comments
K. KEY CONTROL
1. Describe key control system
(a) Who is responsible for issuance of keys?
(1) Are keys signed for?
(b) Are all keys accounted for?
(c) Are issuance of keys recorded?
(1) Is report kept up to date?
(d) Master keys
(1) Number
(2) Name
(3) Position
(e) Are keys removed from vehicles at night and on weekends?
(f) Procedure for return of keys when employee is terminated or transferred?
2. Comments
L. VENDOR AND VISITOR CONTROL
1. How are vendors controlled?
(a) Escorted or issued Badge
(1) Log (sign-in/sign-out)
(2) Permanent (daily) vendors
(3) Periodic vendors
2. How are visitors controlled?
(a) Escorted
(b) Badge
(c) Log
3. Are vehicles inspected?
4. Is a single egress/ingress control point used for all visitors, including vendors, repairmen, etc.?
o Yes o No
5. Is a property pass system used for property removal? o Yes o No
6. Comments
M. CONTRACT PERSONNEL
1. Janitorial service
(a) Contractor

(b) Supervisor's name and address	
(c) How long has service been supplied?	
(d) Work period	
(1) Number of personnel	
2. Contractors working in the facility (not guard, alarm, janitorial)	
NAME & ADDRESS	
TYPE OF WORK	
(a) Do contractor personnel have to sign register when entering or leaving facility?	
(b) Is there an up-to-date list of names and addresses of all contractor personnel?	
(c) Do vehicles of contractor employees that enter the facility have an identifying decal?	
(d) Are the vehicles of contractors inspected?	
(e) Is there an identification system for contractors?	
3. Comments	
N. DISPOSAL	
1. Trash removal	
(a) Name and address of trash removal service	
(b) Is trash periodically inspected?	
(c) How often is trash removed?	
(d) Is trash removed from facility under supervision?	
2. Explain	
3. Comments	
O. EMERGENCY PLANS	
1. Does the facility have emergency plans?	
(a) Bomb Threat o Yes o No	
(b) Fire o Yes o No	
(c) Tornado o Yes o No	
(d) Hurricane o Yes o No	
(e) Flood o Yes o No	
(f) Earthquake o Yes o No	
(g) Explosion o Yes o No	
(h) Loss of utility service o Yes o No	
(i) Civil disorder o Yes o No	
2. Personnel safety	
(a) Safety supervisor	
(b) Are safety plans posted?	
(1) Up-to-date?	
(2) Clear and concise	
3. Is there an Emergency Plan Coordinator? o Yes o No	Name

4. Has the plan been tested? o Yes o No
When?
5. Are drills conducted? o Yes o No
6. Comments
P. OFFICE
1. Mail handling
(a) Who handles mail?
(1) Incoming
(2) Outgoing
(3) Is all mail opened?
(b) Are all package distributed?
(c) Has the individual been instructed about letter bombs and procedures for handling?
2. Is there a facility policy for office procedures?
3. Comments
Q. ALARM SYSTEMS
1. Are alarms used in buildings?
(a) Manufacturer
(b) Type
(c) Date of installation
(d) Serviced by
(e) Date of inspection
(f) What is the procedure for activating and deactivating the system?
(g) What employees are allowed to turn off the alarm system?
R. MISCELLANEOUS
1. Are buildings locked at night?
(a) Who is responsible?
2. Are lights left on in buildings at night?
(a) Type of lighting?
(b) Who is responsible?
3. Are fire stairwells used on a daily basis?
4. Does the facility use elevators?
5. What control is extended over their use?
6. Do elevators connect controlled access floors with public access floors?
7. Comments:

SURVEY CHECKLIST FOR RESIDENTIAL SECURITY AND PERSONAL SECURITY PRACTICES

Area	Yes	No	Remarks
A. GENERAL			
1. Type of residence			
2. Address/location			
3. Name of Requester:			
(a) Organization/office symbol			
(b) Duty phone			
(c) Home phone			
4. Individual(s) conducting survey:			
(a) Name/rank			
(b) Organization/office symbol			
(c) Duty phone			
5. Date of survey			
6. Description of residence			
7. Individual(s) interviewed			
(a) Name/rank			
(b) Organization			
(c) Duty phone			
8. Location of residence			
(a) Urban			
(b) Suburban			
(c) Incorporated			
(d) Unincorporated			
(e) Government installation			
9. Obtain plot plan of residence showing:			
(a) Compass rose showing north			
(b) Perimeter barrier with gates			
(c) Parking areas/facilities			
(d) Any planned remodeling or expansion of residence?			
10. Obtain as-built drawings of the residence showing:			
(a) Construction of exterior/interior walls			

(b) Locations of windows, doors, and skylights			
(c) Location and size of all vents, utility openings, etc.			
(d) Electrical runs, outlets, switches.			
B. EXTERIOR			
1. Is exterior lighting checked regularly and bulbs replaced?			
(a) By whom?			
2.Is exterior fence/wall checked regularly and any breaks or washouts repaired?			
3. Is vegetation cut back near house and exterior wall/fence?			
(a) How often?			
(b) Who is responsible?			
C. BUILDING			
1. Are doors kept locked when at home?			
2. Are exterior doors double locked?			
3. Is there a secondary interior security door that is double locked or has throw bolts?			
4. Is the entrance door(s) solid to the core?			
6. Does the entrance door(s) have dead-bolt locks?			
7. Do the bolts extend at least three-fourths of an inch into the strike plate?			
8. Are the door hinges located on the interior to prevent removal from the outside?			
9. Have the lock cylinders been replaced when first accepting the apartment?			
10. Is there little or no “play” when you try to force the door bolt out of the strike plate by prying the door away from the frame?			
11. Are locks in good repair?			

12. Are all locks firmly mounted?			
13. Can all doors be securely bolted?			
14. Can any of the door locks be opened by breaking out glass or a panel of light wood?			
15. Have all unused doors been permanently secured?			
16. Does adequate lighting exist in the hallways?			
17. Can hallway lights be turned on from inside of the apartment?			
18. Are peepholes installed on doors leading to hallway entrances?			
19. Has an interview grille or one-way viewer been installed on the main door?			
20. Do locks on the balcony doors secure doors adequately?			
21. Can access to the balcony be gained from other apartments, or by climbing drainage pipes or other fixed structures?			
22. Are window frames and locks adequate?			
23. Are window and wall air conditioners and exhaust fans secured against removal?			
24. Are windows left open when no one is home?			
25. Are windows left open when residents are sleeping?			
(a) Do they have grilles or bars?			
(b) Do they have security pins to hold them partially open?			
26. Are interior lights turned off at night?			
27. Are spare keys hidden			

under mat or otherwise near entrance?			
28. Is name of resident on mailbox or near doorbell?			
29. Have ladders, trellises, or similar aids to climbing been removed to prevent entry into second story windows?			
30. Do trees and shrubbery around the apartment afford an opportunity for person(s) to lie in wait undetected?			
31. Do trees and shrubbery around apartments create access to balconies or windows?			
32. Are balcony lights operational and can they be turned on from inside the apartment?			
33. Can access be gained to elevator or utility shafts in the complex, thereby aiding in access through vent windows?			
34. Are roof hatches, trap doors, or roof doors properly secured?			
35. Is outside security lighting adequate?			
36. Are there lights to illuminate the sides of the residence, parking area and entranceway?			
37. Does the main entrance to the apartment complex remain secured when not in use?			
38. Does the apartment require a burglar alarm?			
D. SECURITY PROCEDURES			
1. Are the phone numbers for the local police/security force readily available?			
2. Is there a family dog?			
(a) Does it react to external			

noise?			
3. During extended absences, does someone housesit or check the residence on a daily basis?			
(a) Are lights, radio, or TVs turned on and off automatically by timers in evening?			
4. Are the draperies drawn at night?			
5. Are flashlights located in easily accessible places in case the lights go out?			
6. When the residence is unoccupied during evenings, are lights and radio/TV left on?			
7. Are workmen allowed to be in house or exterior grounds when residents are absent?			
(a) Are workmen scheduled in advance?			
5. Is domestic help checked by security?			
E. SAFEHAVEN			
1. Does safe haven have adequately hardened walls?			
2. Are doors equipped with deadbolt(s), throw-bolts or other similar security devices?			
3. Are doors adequate to provide 15-minute penetration resistance and ballistic protection?			
(a) Describe			
4. Are primary/secondary communications provided?			
(a) Describe			
(b) Do they operate?			
(c) Who do they net with?			
5. Are there the following items available?			
(a) Flashlights?			

(b) Candles?			
(c) Radio?			
(d) Fire extinguisher?			
(e) Firearms and Ammunition?			
(f) Water?			
(g) Telephone directory/emergency numbers?			

F. PERSONAL SECURITY PRACTICES	*YES*	*NO*
1. Have the names and identification of all your credit cards been written down and kept in a safe place?		
2. Do you always lock your car when leaving it?		
3. Do you try to park your vehicle in an area that is well lit?		
4. Do you check your car before you get in? (Look underneath the vehicle, check if it appears as though somebody has been under the hood. Look all the way around.)		
5. Do you frequently check your car safety equipment and keep the gas tank one-fourth to one-half full?		
6. Do you avoid carrying keys that are attached with your identification?		
7. Do you try to carry the minimum amount of cash that you expect that you will need?		
8. Do you avoid being flashy and flamboyant? (It is suggested that we try to blend in with the local community as much as possible. Avoid wearing your favorite NFL team jacket and similar items.)		
9. Do you usually go shopping with at least one other person? (It is often hard to avoid large crowds in this area, but when in the community, try to stay away from areas of unrest. Such areas would be locations holding political rallies, demonstrations, or even people having loud arguments.)		
10. Do you keep your keys readily available when approaching your apartment door? (It is suggested that upon walking up to your apartment, your keys should be in your hand and be ready to put into the lock. This eliminates having to take a lot of time looking for your keys and therefore giving someone the opportunity to attempt to rob or attack you.)		
11. When you are walking down the streets of the city, are you conscious of what is going on around you? (Many victims of terrorist or criminal attacks have merely wondered into the target area. In time you will know what looks out of place, so if something feels wrong leave the area.)		
12. Are you alert to potential surveillance and constantly vigilant? (Don't be paranoid, but do look around. See if somebody is following you, or watching where you are going. A typical terrorist tactic is to follow the target for a few days (or even weeks) to see what habits they have.		

13. Do you open the door for people you don't know or don't expect? (In some countries, maids seeking employment will be ringing your bell all the time. If you want one, ask friends who they have, and check their references before making a choice. Never let maids in who come door-to-door; they often are looking for what you have in the house so that they can send someone back for it.		
14. When people ring your apartment buzzer, are they denied admittance until their identity and purposes for the visit are known?		
15. Is your name listed on the buzzers located at the apartment entrance? (When in a foreign country (especially in a high threat area), it is not a good idea to put your name on the apartment buzzer. It is suggested that you use another name or what your name would be in the local language.)		
16. Do you know the other Americans that live in the building? (It is suggested that each person get to know who his or her immediate neighbors are. This way one can become familiar with the people that come and go throughout their floor as well as the entire building. Also, consider keeping a list of all your neighbors' telephone numbers for emergencies.)		
17. Do your neighbors have your phone number?		
18. Are you aware of local command policy regarding the wear of uniform items in public? (In certain countries, restrictive policies are in effect.)		
19. Are family members familiar with the local area, alert to instances of possible surveillance, and aware of what countermeasures to take?		
20. Are their adequate plans in the event a burglar is surprised in the home?		
21. Do you avoid keeping a "hidden" key outside of your apartment?		
22. Do you instruct your children in personal safety measures, particularly those that apply to children who walk to and from school alone?		
23. Are children instructed in correctly handling telephone calls from strangers?		
24. In case of a fire at night, do you keep extinguishers readily available?		
25. When departing for work and returning, do you vary the routes (particularly in the vicinity of your residence and work area)? (Every effort should be made to avoid setting predictable patterns. Varying your routes and departure/arrival times serves to complicate terrorists planning and may cause the would-be attackers to seek a "softer" target.		
NOTE: The items in this checklist are not all-inclusive and should be used only as a guide by individuals conducting surveys. Many additional and valuable observations may emerge from examining the local physical environment and discussing personal behavior patterns with the subjects of the survey.		

SECURITY SURVEY WORKSHEET FOR HIGH-RISE COMMERCIAL BUILDINGS

Area	Yes	No	Remarks
A. PRE-SURVEY INFORMATION AND MATERIAL TO BE OBTAINED			
1. Location and address of building			
2. Date of survey			
3. Name and title of person interviewed			

NOTE: Procure plot plan of first floor, basement, and any other floors which differ in comparison to the design of the other floors. It may suffice to have a plan of only one floor above the first if all others are similar and contain no unique areas or features as they relate to security. Do not overlook floors reserved for service equipment.

4. Describe the entire premises being surveyed.			
5. Is the premises a single building, or is there more than one building involved?			
6. How do these buildings relate to each other?			
7. How far apart are they?			
8. Do they connect?			
9. Are there any outside grounds involved?			
10. Are there any connecting parking areas either inside or outside the building complex?			
11. What types of tenants does the building house?			
(a) Retail stores?			
(b) Business offices?			
(c) Professional offices?			
(d) Banks?			
12. Is there one major tenant in the building?			
13. How many floors does this tenant occupy?			
14. If this is significant, which floors are these?			
B. SECURITY AT STREET LEVEL AND BELOW			
1. How many doors are there at street			

level used by pedestrians?			
2. Describe their location and designation, and mark them on the plot plan.			
3. Are there any other doors at street level, such as, delivery, fire exit doors, etc.?			
4. Describe their locations and designations.			
5. How are these doors protected against illegal use when closed?			
6. How are these doors controlled when open?			
7. How many windows are there at ground level or below?			
8. How are these windows protected against illegal use?			
9. Could any window be opened or removed from the outside?			
10. Does the building have a sidewalk elevator?			
11. What security is provided when the elevator is in use?			
12. How is it secured when not in use?			
13. Are there any storm sewers or utility tunnels entering or running under the building?			
14. Are these of such a size (96 square inches) or so located as to permit illegal entry?			
15. If so, how can they be protected to deny such entry?			
C. LOBBY			
1. Open periods			
(a) During what hours is the lobby open to the general public?			
(b) Is any control exercised over personnel movement during this time?			
(c) Is it possible to have any personnel control in the lobby during open periods?			
(d) Describe the controls in force.			
(e) What advantages would added			

controls have?			
(f) How many banks of elevators are there in the lobby?			
(g) Are there any controls exercised at the elevator?			
(h) Do all or part of the elevators descend to lower floors?			
(i) What levels do they serve?			
(j) Are special elevators used for freight?			
(k) Do these open into the lobby?			
(l) Is there direct access to freight elevators from outside the building or from loading docks?			
(m) If yes, is any type of protection provided against surreptitious use of such elevators from these areas?			
(n) Are elevators manually or automatically operated?			
(o) Are there any special elevators which service parking areas only, stopping at the lobby level only?			
(p) Are the elevators or escalators supervised?			
(q) To what extent?			
(r) Do doors from fire stairways leading to upper floors enter the lobby or floors below?			
(s) What form of protection is provided against illegal entry from outside through these doors?			
(t) Are there any open stairways to lower or upper levels of the building?			
2. Closed periods			
(a) During what hours, if any, is the building open to tenants but closed to the general public?			
(b) How are doors and other openings controlled during these semi-closed periods?			
(c) Is there any control over tenants' entering or leaving when the building is closed to the general public?			
(d) How are these persons			

identified and checked in and out?			
(e) Are equipment repairmen permitted in the building during these semi-closed periods?			
(f) How are these persons controlled?			
(g) Are there any rules pertaining to the removal of equipment, packages, etc., during these periods?			
(h) Is there any time that the building is closed to both public and tenants?			
(i) How is this accomplished?			
(j) Is there a procedure established to admit tenants, workmen, etc., on an emergency basis when the building is completely closed?			
3. Custodial personnel			
(a) Is the custodial work in the building done by building employees or by contract personnel?			
(b) During what hours do custodial personnel work?			
(c) How is this service supervised?			
(d) Do custodial personnel have keys to the various areas?			
(e) Do any tenants have their own custodial or maid service?			
(f) If yes, answer the following questions:			
(1) During what hours do custodial personnel or maids work?			
(2) How is this service supervised?			
(3) Do custodial personnel or maids have keys to the various areas?			
(g) How are custodial pass keys controlled?			
(h) Is trash removed by custodial personnel or maids?			
(i) How is this done?			
(j) Is there any control exercised over the entering and leaving of			

custodial personnel or maids?			
(k) How is this accomplished?			
(l) Is there a package-inspection system in force to cover custodial personnel or maids when they leave the building?			
D. BUSINESS FIRMS IN THE BUILDING			
1. Are there any retail business firms in the building?			
2. Are they confined to the street floor and below?			
3. Are the areas occupied by these firms to be included in the survey?			
4. Do these businesses affect the security of the building when other parts of it are closed?			
5. Are there any businesses or professional offices that have to be open to the public during normally closed or semi-closed hours for the building?			
6. How does this affect the overall security?			
7. How is it handled?			
8. Are any of the business establishments or offices protected by separate anti-intrusion alarms when closed?			
9. Do security personnel have any responsibility in connection with these alarm systems?			
E. BASEMENTS, SUB-BASEMENTS, AND PARKING			
1. How many levels of operating area are there in the building below ground?			
2. How is entrance made to these areas from outside?			
3.Are equipment rooms, power rooms, shops, and storerooms locked when not occupied by operating personnel?			
4. Does the building have sub-level parking?			
5. How many levels are there?			

6. Is this for tenant parking only, or is it open to the public?			
7. How is the parking facility operated or controlled?			
8. What are the lighting conditions in the parking levels?			
9. Do security personnel tour parking levels?			
10. How are entrances and exits to parking areas controlled?			
11. During what hours are they open?			
F. ROOF AREAS			
1. Does any part of the roof of the building permit entry to the building by crossing to the roof from the roof of another building?			
2. How are exits from the building to the roof controlled?			
3. Have any measures been taken to deny access to the roof from adjacent buildings?			
4. Is the roof of the building used for personnel activities, such as swimming, dancing, other forms of recreation, restaurants, observation, etc.?			
5. If so, how is the roof protected against fire?			
6. Is a fire inspection made of roofs when special activities are completed or when the building is semi-closed or closed?			
7. How soon after special activities or when the building is semi-closed or closed does this inspection take place?			
G. FIRE PROTECTION			
1. Is the building equipped with a sprinkler system?			
2. Is the entire building so protected?			
3. If no, what areas are covered or not covered, whichever is greater?			
4. If the entire building does not have sprinklers, is there any type of fire detection used?			

5. Describe the fire-protection system, and indicate those parts of the building that have no automatic protection.			
6. How many risers feed the sprinkler systems?			
7. Are the risers equipped with water flow alarms?			
8. Are alarms local, proprietary, or central station and/or connected to the fire station?			
9. Is the building equipped with an audible local alarm system to alert tenants?			
10. Is this a coded system to designate which floor the alarm came from?			
11. Are the alarms loud enough and so located to alert all tenants in the building?			
12. Is the first alarm silent except to building management employees, who in turn must sound the general alarm manually if required?			
13. Are there manual fire-alarm pull boxes located strategically on each floor of the building?			
14. Is each floor of the building equipped with one or more fire hoses in wall cabinets or racks?			
15. Is each floor of the building equipped with a number of strategically located fire extinguishers?			
16. If yes, are these extinguishers regularly inspected or conditioned?			
17. Are the hose lines connected to those risers used for the sprinkler system?			
18. Is water pressure in the risers on all floors sufficient to handle both sprinklers and hoses?			
19. If no, is the building equipped with fire pumps to keep pressure in these lines high enough to be effective?			

20. Where are these pumps located?			
21. Who is responsible for these pumps?			
22. How often are these pumps tested?			
23. Are fire-hose valves at each hose station tested regularly?			
24. Is the fire hose and play pipe tested to ensure it is not rotted, cut, or obstructed?			
25. Are there any firewalls dividing floors of the building?			
26. If so, are openings between protected by fire doors?			
27. Are the fire doors normally open or closed?			
28. If open, are they equipped with automatic closures (magnetic releases) that would activate if a fire occurred?			
29. Is the building equipped with fire escapes or fire stairwells?			
30. If fire stairwells are used, are they equipped with fans to bring air from outside to build up positive air pressure and prevent smoke from seeping into them during fires?			
31. Are fire stairwells compartmented to protect against smoke seepage?			
32. Are fire doors to fire stairwells made of fire-resistant or fireproof material?			
33. Are these doors equipped with approved panic hardware?			
34. Are these doors kept closed at all times?			
35. If kept open, are these doors equipped with the closures, (magnetic releases) which will operate if fire occurs?			
36. Does each floor of the building form a compartment that would effectively block fire from spreading to other floors?			
37. Are air conditioning and ventilating			

flues equipped with dampers that would close automatically in case of fire?			
38. Are these dampers regularly maintained and tested?			
39. Are openings where water pipes, wires, etc., pass through solid walls sealed to eliminate smoke seepage from other areas?			
40. If the elevators are contemplated for use during a fire, are the shafts sealed or equipped with pressure fans to raise positive air pressure to force out smoke?			
41. If elevators are to be used for evacuation, is there a plan for an orderly method of evacuating each floor?			
42. Does the fire department have ladder trucks and will they reach the top floors and roof of the building?			
43. If no, are procedures in place for helicopter evacuation from the roof, and is it adequate for the tenant population?			
44. Are certain elevators set aside for use by the fire department?			
45. Are all OS&V valves in the risers in an open position and sealed?			
46. How many public fire hydrants are available within a city block in any direction from the building?			
47. How many fire department hookups are there on the outside of the building?			
48. Are the trash containers in service hallways, closets, and maintenance areas properly covered and of metal construction?			
49. Are the boiler room and other maintenance areas properly policed?			
50. Is all combustible trash either immediately removed or safely stored to avoid fires?			
51. Are combustibles, such as paint,			

oil, gasoline, etc., stored in the building?			
52. Is all fire-fighting equipment inspected regularly?			
53. Is a record of inspection maintained?			
54. Are clear and concise instructions posted for the use of fire extinguishers and hoses?			
55. Are fire extinguisher and hose locations properly marked so that tenants can easily locate them during a fire?			

ADDITIONAL NOTES

ENCLOSURE 1 TO TAB B TO APPENDIX 6 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
PORT CHECKLIST (U)

USNORTHCOM SECURITY ASSESSMENT SURVEY FORM AND CHECKLIST FOR NON-US MILITARY PORTS

The following survey form and checklist are provided to assist in conducting security assessments of port facilities. This checklist should be used in conjunction with the guidance in Appendix 6, Tab B of the USNORTHCOM AT OPORD. When completed, the information should be marked, as a minimum, "FOR OFFICIAL USE ONLY".

Name of Port Assessed (include country identification):

_____

Note*: Describe those items, as they are now observable. If an observable situation will change with the arrival of a ship, comment only if included in a SOFA or other presently written, approved agreement or plan(s). "Verbal" reassurances may be noted, but should not be addressed as "fact".*

Date(s) of Assessment:	
Assessment Team Member(s) (include contact information)	
Name	**Contact Information**
1.	
2.	
3.	
4.	
5.	

SECTIONS

I PERSONS INTERVIEWED/CONTACT INFORMATION POC LIST
II THREAT INFORMATION
III DETAILED PORT INFORMATION
IV FACILITY ENGINEERING
V SECURITY FORCES
VI DIVING OPERATIONS/ANTI-SWIMMER
VII PORT SERVICES/HUSBANDING AGENTS
VIII SECURITY PLANNING AND PROCEDURES
IX AIR FACILITIES (See In-transit Airfield Assessment Checklist posted on this homepage.)

SECTION I
PERSONS INTERVIEWED/CONTACT INFORMATION

Name of Port Assessed:_____

Dates:_____

NAME	TITLE/POSITION	CONTACT INFORMATION/ ADDRESS/TELEPHONE NUMBER (S), ETC.

SECTION II
THREAT INFORMATION

Name of Port Assessed:_____

Dates:_____

Note: As applicable during the assessment, add notes regarding expected changes of personnel and circumstance.

ASSESSMENT MEMBERS COMPLETING THIS SECTION:

NAME	CONTACT INFORMATION/TELEPHONE NUMBER (S)

PERSONS INTERVIEWED FOR THIS SECTION:

NAME	TITLE/POSITION	CONTACT INFORMATION/ ADDRESS/TELEPHONE NUMBER (S), ETC.

UNCLASS THREAT INFORMATION

1. General threat assessment (at the UNCLASSIFIED level):

2. Threat Level:

3. FPCON (or comparable security posture) in effect:

4. NCIS Threat Assessment Message DTG.

5. Any threat information developed during the assessment?

FOREIGN FLAG VESSELS

1. Will foreign flag vessels be co-located with U.S. ships?
If Yes, provide comments regarding type and proximity:

2. Will foreign crewmen transiting nearby areas of concern to U.S. ships?

3. Will foreign cargo be off-loaded/on-loaded and/or stores be co-located with U.S. cargo/supplies?

SECTION III
DETAILED PORT INFORMATION

Port/Base/Pier/Anchorage/Fleet Landing/Seaman Centers:_____

GENERAL GUIDANCE: ***This section should be filled out with the intent to include all possible areas and buildings where there will be an identifiable U.S. military presence. Each item identified below should be assessed further using additional sections of this checklist as applicable. (Note: Section VII will describe in more detail places of interest while on liberty.) Redundancy has been built into the sections to facilitate maximum coverage of all areas of concern. Each section should filled out by multiple team members.***

Dates: _____

ASSESSMENT MEMBERS COMPLETING THIS SECTION:

NAME	CONTACT INFORMATION/TELEPHONE NUMBER (S)

PERSONS INTERVIEWED FOR THIS SECTION:

		CONTACT INFORMATION/

NAME	TITLE/POSITION	ADDRESS/TELEPHONE NUMBER (S), ETC.

NOTE*:* ***This portion of the section should reflect all items of interest related to Physical Security. Indicate Host Nation Military and/or Commercial operated. Describe those items, as they are now observable. If an observable situation will change with the arrival of a ship, comment only if included in a SOFA or other presently written, approved agreement or plan(s). "Verbal" reassurances may be reported, but should not be addressed as "fact".***

DETAILED PORT DESCRIPTION:

1. Port:
   a. Location:
   b. Name/address/designation:

2. Pier Description: (List and provide input for each pier U.S. Ships use)
   a. Location:
   b. Name/address/designation:

3. Fleet Landing: (List and provide input for each Fleet Landing U.S. Ships use)
   a. Location:
   b. Name/address/designation:

4. Anchorage Description: (List and provide input for each Anchorage U.S. Ships use)
   a. Location:
   b. Name/address/designation:

5. Seamen Center Description: (List and provide input for each Seaman Center U.S. Ships use)
   a. Location:
   b. Name/address/designation:

6. Documents Obtained: (List and provide input for each)
   a. Chart(s)
   b. Overall diagrams, layouts, Aerial Photograph
      (1) Port(s)
      (2) Harbor(s)
      (3) Pier(s)
      (4) Fleet Landing site(s)
   c. City maps

d. Tidal current flow diagram(s) (direction and speed)
e. SOFAs/other agreements
f. Photographs of the site(s)
g. Blueprints/Floor plans
h. Other (describe)

7. Port usage: (indicate all that apply)
a. Permanent HN Military Base. If so, describe the primary mission of the military port?
b. Transient U.S. Ships:
(1) Where Moor/Anchor?
(2) Logistic support?
(3) Exercises?
(4) Other (describe):
b. Commercial Vessels:
(1) General Cargo
(2) Fuel/POL
(3) Passenger
(4) Fishing (commercial)
(5) Pleasure
(6) Other (describe)

8. Fixed mooring berths: (Note: describe only those with a direct application to visiting U.S. ships, taking note of force protection concerns of nearby berths.)
a. General locations:
(1)
(2)
(3)
b. General commercial berths:
(1)
(2)
(3)
(4)
c. Tanker berths:
(1)
(2)
(3)
(4)
(5)
d. Naval berths:
(1)
(2)
e. Passenger terminals:
(1)
(2)
(3)

f. Bulk cargo areas:
   (1)
   (2)
   (3)
   (4)
   (5)
g. Other (describe)
   (1)
   (2)
   (3)
   (4)

9. Area surrounding the port (describe): (Taking note of force protection concerns of nearby area for tab V and IV.)
   a. Industrial?
   b. Urban (include estimated population)?
   c. Open terrain, hillside, high-rise buildings, etc?
   d. What is the history and degree of oily waste on the water's surface?

10. How far is the Next nearest: (Give brief description including routes and most feasible means to transport personnel and equipment.)

Commercial airfield

Host Nation military airfield and/or installation

US military airfield and/or installation

Commercial hospital

Host Nation military hospital

US hospital

SECTION IV
FACILITY ENGINEERING

Port/Base/Pier/Anchorage/Fleet Landing/Seaman Centers: _____

(NOTE: If this section is completed independently by more than one team member, all inputs should be consolidated into one file/document for submission to the PVAT Program Manager.)

Date(s): _____

ASSESSMENT MEMBERS COMPLETING THIS SECTION:

NAME	CONTACT INFORMATION/TELEPHONE NUMBER (S)

PERSONS INTERVIEWED FOR THIS SECTION:

NAME	TITLE/POSITION	CONTACT INFORMATION/ ADDRESS/TELEPHONE NUMBER (S), ETC.

Note*:* This section should be referenced for each item listed in Section III, especially Medical Facilities. Note: Describe those items, as they are <u>now observable</u>. If an observable situation will change with the arrival of a ship, comment <u>only</u> if included in a SOFA or other presently written, approved agreement or plan(s). "Verbal" reassurances may be included, but should not be addressed as "fact".

PIER/WHARF CONSTRUCTION

1. Construction materials (e.g., reinforced concrete, reinforced concrete frame, reinforced masonry, brick, metal, wood, stone, etc.):

2. Is the pier solid construction all the way to the sea bottom? Describe its construction (e.g., solid, pilings, utility access covers (man accessible) in the pier, etc.)

3. Pier/Wharf
   a. Length:
   b. Width:
   c. Height:

4. Are utility accesses available within the pier?
   a. If "Yes", are any "man accessible" (over 96 square inches)?
   b. If "man accessible", are the covers secured and/or the utility tunnels otherwise rigged to prevent access?

   Comments:

5. Were pier/fleet landing blueprints available?
   a. If available, were they reviewed?

b. Comments:

LIGHTING

(Notes: In most civilian ports, "sufficient lighting" may be a relative term. For the purposes of this assessment, "sufficient" is where lighting lends the ability to immediately limit/reduce shadowed areas to assist patrols, permit the ready identification of personnel at 100 feet or more, and to check identification without strain at 3 feet or greater.)

1. Lighting availability:
   a. Is lighting available on the pier/wharf/landing platform?
      (1) If "Yes", is the lighting sufficient?
      (2) Comments:
   b. Under deck lighting:
      (1) If "Yes", is the lighting sufficient?
      (2) Comments:

2. Is emergency/portable lighting available?
   a. If "yes", describe (include where presently staged, and expected time that equipment could be rigged/activated)
   b. Comments:

3. Does the protective lighting for this port meet adequate intensity requirements?

4. Are the zones of illumination from the lamps directed downward and away from guard personnel?

5. Is perimeter protective lighting utilized so that security patrol patrols remain in comparative darkness?

6. Are lights checked frequently for proper operation?

7. Do light patterns overlap to compensate for burned-out lamps?

8. The above protective lighting questions extend to any contiguous body of water. Are these areas provided lighting as well (including waterlines)?

9. How is lighting operated (e.g., automatic (photocell), manually, etc.)?
   If "Manually", who is responsible for operating the lights?

10. In the event of problems with the lighting, who may be contacted for repairs and/or other assistance (include name/position and telephone number)?

11. Are the zones of illumination directed downward and away from guard personnel?

12. Is emergency signal lighting available (e.g., strobes, pyrotechnics, etc.)?

ELECTRIC/POWER

1. What is the source/location of primary power, transformers (voltage, amperage)?

2. Is/are backup power system(s) available?
   a. If "Yes", describe (including type, staged location and approximate time to have rigged and activated, fuel required, battery life):
   b. Would backup power be sufficient to meet expected needs (numbers and power output)?
   c. Are backup power sources protected (including the system(s), transmission lines, fuel lines/sources, etc.)?
   d. Are person(s) on each shift capable of operating the backup system(s) and/or know the process to recall operators?

3. Are security measures in effect to protect port electrical power facilities?

PORT FACILITIES/BUILDINGS

1. Building specifics:
   a. Buildings in the port: (Attach a drawing/map layout of the port, if available)
   b. Purpose or use of key structures:

2. Predominant construction materials of key buildings: (brick, concrete, wood, steel, mason blocks)

3. Number of entrances/exits to port/pier area:
   a. Number of vehicular entrances/exits:
   b. Number of pedestrian entrances/exits

4. Describe the intervening distance between perimeter barriers and the nearest structure (internal or external), i.e., Open cleared flat land etc.

5. Are windows alarmed, grilled, and shatter resistant with protective window film?

6. Is their adequate exterior lighting and does it overlap to compensate for burn out?

7. Are outdoor accesses, such as fire escapes, roofs, doors, air vents, etc. secured?

8. Can the facility act as a safe harbor in an emergency?

INTRUSION DETECTION SYSTEM (S) (IDS)

1. Are CCTV and/or motion detection systems employed and operational?

If "Yes", describe generally:

2. Is IDS (if any):
   a. Local?
   b. Proprietary?
   c. Police Dispatch connection?

3. Is IDS and/or CCTV available on:
   a. The perimeter?
   b. The pier/wharf?

4. Is backup power available for any installed IDS?
   If "Yes", describe (e.g., generator, batteries (or a combination), UPS, etc., and whether automatic, manual, estimated operating time, etc.)

5. Is the CCTV system "record capable?"

6. Does the port have a generalized alerting system (PA, "Giant Voice," etc.)? If no, how is US/HN Security alerted?

FIRE SERVICES

1. Where is the nearest fire department?

2. Is the Fire Department capable of providing assistance to ships?

3. What is the fire department estimated response time to this port/pier (include any substantial differences in day and night response)?

4. Are their Fire Fighting Craft in the area and what is there day and night response time?

5. How high can the fire department ladder equipped platform reach?

6. To what extent is oily waste (degree and size of sheen) on the water's surface?

7. Is the port/pier equipped with an audible local fire alarm to alert occupants?
   a. Does the alarm system enunciate at a central control desk that identifies the exact location/pier of the incoming alarm?
   b. Is the system periodically tested?
   c. Are fire alarm pull boxes located on each pier?
   d. Does each pier have an appropriate number of fire extinguishers?
   e. Are these extinguishers checked and serviced accordingly?
   f. Are piers equipped with Fire mains? If so, are they compatible with shipboard FF equipment? What sizes are there and are adapters required?

SECTION V
SECURITY FORCES

Port/Base/Pier/Anchorage/Fleet Landing/Seaman Centers:_____

(NOTE: If this section is completed independently by more than one team member all inputs should be consolidated into one file/document for submission to the PVAT Program Manager.)

ASSESSMENT MEMBERS COMPLETING THIS SECTION:

NAME	CONTACT INFORMATION/TELEPHONE NUMBER (S)

PERSONS CONTACTED FOR THIS SECTION:

NAME	TITLE	CONTACT INFORMATION/ ADDRESS/TELEPHONE NUMBER (S), ETC.

Note: ***This section should be REFERENCED for each Item listed in Section III, Especially Medical Facilities. Also attention should be paid to the routes necessary to get to/from point A to point B. Note: describe those items, as they are now observable. If an observable situation will change with the arrival of a ship, comment only if included in a SOFA or other presently written, approved agreement or plan(s). "Verbal" reassurances may be included, but should not be addressed as "fact".***

SECURITY PERSONNEL

1. Describe the composition of the security force at this port? (Primary force, backup force and ASF, civilian force)
   a. US Military
   b. US Contract
   c. DoD Police
   d. HN Military
   e. HN Police
   f. HN Contractors
   g. Other (describe):

2. Are bomb squads available?
   If "Yes":
   a. Where are they located?
   b. What type of equipment do they have at their disposal?
   c. What is the estimated response time?
   d. Are bomb-trained dogs available?
      If "Yes":
      (1) How many?
      (2) Where are they located?
      (3) If needed, what is the estimated response time?
      (4) How may their services be arranged?
      (5) Do they pre-sweep ship's assigned berths and/or fleet landing areas prior to U.S. Ship's use? Can this be arranged?
   e. Are EOD divers available?
      If "Yes", how may their services be arranged?

3. Is the US/HN security force training up to date?
   (Personal observation, if possible, may be necessary)

   2. Is the US/HN security force armed?
   If "Yes", describe the weapon(s) carried and is there use of deadly force training:

5. Do US/HN security forces cover a 24-hour period?

6. Is security watch times and patrol route times varied to break routine cycles?

7. How many posts are required to be manned when U.S. Ship is in port?

8. Do US/HN security forces wear distinctive uniforms? (Describe)

9. Are police/security response vehicles readily identifiable?

10. What percent (estimated) of HN security forces speak English? (Try to give a feel of what to expect as far as communicating in general)

11. Do security personnel patrol the perimeter?

12. In making rounds throughout the port, do security personnel record their presence at key locations in the port (e.g., portable watch locks, telephones, radios, etc.)?

13. Is there a HN quick reaction force (QRF) available?
    If "Yes":
    a. What type(s) of force(s) are available (e.g., riot control, SWAT, etc.)?
    b. Are they on duty, on call, etc.?
    c. What is the minimum response time for each?

14. What rules of engagement and/or limitations on use of force are in effect?

15. What "Hazmat" capability does the port have?

WATERSIDE SECURITY (Applies both at anchorage and pier side)

1. What is the agreed waterside standoff distance?
   a. Is there an agreed reaction zone?
   b. Is there an agreed engagement zone?

2. Does the host nation/coalition security provide support on the waterside of this site?

3. What additional security measures are implemented for those vessels at anchorage or pier side?
   a. Who provides this service?
   b. Describe:

4. What type(s) and numbers of watercraft are involved in the port security mission? (Describe the operating agency, and types and numbers of patrol watercraft available)

5. Patrol watercraft:
   a. Do patrol craft enforce the designated standoff?
   b. Do they contact and escort?
   c. What are their tactical response procedures?
   d. How are communications established if the ship desires the investigation of another craft, senses trouble, etc?

6. Aside from patrol craft, what waterside physical security measures are in place?
   a. Standoff markers/buoys/floats?
   b. Signs?
   c. Anti-swimmer nets?
   d. Log or other booms?
   e. Barges
   f. Other (describe):

7. To what extent is oily waste (degree and size of sheen) on the water's surface?

SECURITY COMMUNICATIONS

1. Do watercraft and/shore security forces craft have communication with shore based HN and shipboard security forces? (If "Yes", describe the system used, telephone numbers, frequencies, etc.)
   a. Picket boats:

b. Shore Patrol:
c. Beach Guard:
d. Water taxi(s):
e. Other (describe):

2. Do communications system(s) have an encryption capability?

2. Are communications centers protected?

4. Are U.S. security allowed top use their own radios and frequencies?

SURVEILLANCE SYSTEMS

1. Is there a surveillance/early warning capability at the port?
If “Yes”, describe:

2. Is there surface search radar (whether Port Authority/ship, etc.)?
If “Yes”, describe:

3. Are there acoustic underwater sensors available?
If “Yes”, describe:

2. Are there observation positions with day/night optics?
If “Yes”, describe:

SHORE PATROL/BEACH GUARD

1. Will Shore Patrol and/or Beach Guard be permitted?

2. Do the HN security forces prefer Shore Patrol and/or Beach Guard be in uniform or civilian clothing?

2. Will a HN police representative accompany or be posted with the Shore Patrol and/or Beach Guard?

SECTION VI
DIVING OPERATIONS/ANTI-SWIMMER

Port/Base/Pier/Anchorage/Fleet Landing/Seaman Centers:_____

Dates:_____

ASSESSMENT MEMBERS COMPLETING THIS SECTION:

NAME	CONTACT INFORMATION/TELEPHONE NUMBER (S)

PERSONS CONTACTED FOR THIS SECTION:

NAME	TITLE/POSITION	CONTACT INFORMATION/ ADDRESS/TELEPHONE NUMBER (S), ETC.

Note: ***Describe those items, as they are now observable. If an observable situation will change with the arrival of a ship, comment only if included in a SOFA or other presently written, approved agreement or plan(s). "Verbal" reassurances may be included, but should not be addressed as "fact".***

DIVING OPERATIONS/NAVIGATION

1. What is the range of tides and general impact on the ability of the ship to get underway? (Shallow water or low bridges)

2. Is the anchorage(s) or the ship's berth within 500 meters (550 yards) of any of the below?
   a. Small boat traffic areas?
   b. Fishing boat areas?
   c. Marinas?
   d. Shipping lanes?
   e. Restricted channels?
   f. Shoal water?
   g. Submerged hazards?

3. Diving and Salvage response concerns:
   a. What is the local Host Nation (HN) diving, salvage and EOD diving capability?
   b. Is there space at the site for staging diving and salvage equipment, either HN or USN?
   c. What is the height above water for dive areas?
   d. Are there any boat ramps in the vicinity of the port/pier?

e. Where is the closest operational hyperbaric chamber and is their Medevac capability?
f. What is the Speed and direction of the currents and the times it changes direction?

ANTI-SWIMMER/DIVER

1. Are there dedicated anti-swimmer operations while warships are present?

2. Can the ship/site be easily inspected at the waterline?

3. Is their adequate lighting of the site waterline area for anti-diver and anti-swimmer surveillance? If Yes, describe.

4. Does the site have tunnels, passages or other underwater enclosures or openings that could be used by terrorist divers or swimmers as hiding places, etc.? If Yes, describe.

5. Are there any nearby areas that could be used as covert water entry points for terrorist divers or swimmers? If Yes, describe.

6. What are the typical currents in the vicinity of the anchorage or berth?

7. How does the currents impact potential terrorist diver and swimmer operations?

8. What is the clarity of the water and impact on anti-diver and anti-swimmer surveillance?

9. Are there any nearby sport scuba operations that could be used as a guise for terrorist swimmer or diver operations? If Yes, describe.

10. Does the pier have any ladders, steps or handholds that could assist terrorist divers or swimmers? If Yes, describe.

11. Is there an EOD dive capability at the port?
    a. Where are they located?
    b. What is their response time?
    c. Can (or will) EOD conduct sweeps of the pier before the ship's arrival?
    d. Can (or will) EOD conduct period sweeps of the pier and/or hull while at berth or anchorage?

SECTION VII
PORT SERVICES/HUSBANDING AGENTS

Facility: _____

General Guidance: ***One copy of this section should be filled out by the Husbanding Agent and submitted to the PVAT. The PVAT is responsible for there own submission. This will give a wider scope of data input.***

Note*: Describe those items, as they are <u>now observable</u>. If an observable situation will change with the arrival of a ship, comment <u>only</u> if included in a SOFA or other presently written, approved agreement or plan(s). "Verbal" reassurances may be included, but should not be addressed as "fact".*

Dates: _____

ASSESSMENT TEAM MEMBERS COMPLETING THIS SECTION:

NAME	CONTACT INFORMATION/TELEPHONE NUMBER (S)

PERSONS CONTACTED FOR THIS SECTION:

NAME	TITLE/POSITION	CONTACT INFORMATION/ ADDRESS/TELEPHONE NUMBER (S), ETC.

CONTRACTOR SERVICES:

1. Are the Husbanding Agents, contractors and sub-contractors screened? If "Yes", describe:

2. Is there a restriction on inspecting tugs/support vessels before them approaching the ship?

3. Are camels or other breasting out devices in good condition and can they be inspected by U.S. and/or local authorities?

4. Is another vessel required for any hotel services and who is the service provider (e.g., CHT, fuel, trash, water, refuse donuts, water taxis; Husbanding Agent, etc.)? If Yes, Describe each and who controls coordinating its services?

5. Who controls access to these vessels?

6. Is there a list that identifies these vessels (i.e., hull numbers) and can this list be obtained?

a. Can the hours of operation for these vessels be regulated?

7. Are security measures in place to protect hotel services (e.g., electrical power, communications, water, etc.)?

8. Are visitors required escorts onto restricted areas?

a. Are protective barriers available for Ships? If Yes, describe. (Size, type, etc.)

9. Are reports and complaints handled quickly by HN/Port Ops?

10. Does limited number of roads restrict accesses to the port? Describe.

11. Is assess to the port is limited to water borne vessels?

12. Are their other sources of choke points that can restrict the recall of personnel (railroads, draw bridges, tunnels)?

LIBERTY PARTIES ASHORE

1. Are there a wide number of places for personnel to gather when on liberty (towns, cites, beaches)? If “Yes”, describe each in detail:

a. Are any locations on a local restricted list and why?

2. Is there a wide range of types of places for personnel to gather on liberty (bars, restaurants, shops, etc.)?

3. Do U.S. Ships utilize a Seaman Center while in port? If yes, describe the facility.

4. Should liberty parties be stranded ashore and/or otherwise unable to return to the Ship for any reason, is there a place they can go for refuge? If “Yes”, describe:

5. Is the distance to gathering places problematic for regular travel to and from the Ship?

6. Are bus stops:
   a. Varied from Ship-to-Ship?
   b. Identified by the Ship's name or other ready identifier?

7. Are tour buses identified with the Ship's name?

8. Is the distance to gathering places problematic for regular travel to and from base? Will shore patrol be adequate to provide security? If not, what degree of U.S. HN support will be required?

SECTION VIII
SECURITY PLANNING AND PROCEDURES

Port: _____

Dates: _____

ASSESSMENT TEAM MEMBERS COMPLETING THIS SECTION:

NAME	CONTACT INFORMATION/TELEPHONE NUMBERS

PERSONS INTERVIEWED FOR THIS SECTION:

NAME	TITLE/POSITION	CONTACT INFORMATION/ ADDRESS/TELEPHONE NUMBER (S), ETC.

PLANNING

1. Has a Security Officer been assigned to this port to specifically address physical security, FP, and/or loss prevention issues?

2. Does the port have a physical security plan?
   If "Yes", what is the date of the plan?

3. Does the plan contain:

a. Measures to reduce the opportunities for the introduction of bombs?
   If “Yes”, describe:
b. Procedures for evaluating and handling bomb threats?
c. Policies and plans for the evacuation of personnel?
d. Bomb search procedures?

4. Does the port have a counter-sabotage program?
   If “Yes”, does the program include:
   a. Access control to mission-essential sites?
   b. Specific checks of mission-essential sites/equipment by patrol personnel?

   2. Have specific “restricted areas” been designated in writing in the plan?

SURVEYS AND ASSESSMENTS

1. Are threat assessments (TAs) of the port conducted periodically?
   If “Yes”:
   a. What is the date of the last TA?
   b. Who did the assessment?
   c. How often are they conducted?

2. Has the Security Officer (or other responsible person) conducted a “risk analysis” (RA) concerning the local terrorist and/or criminal threat?
   a. What is the date of the last RA?
   b. Who did the analysis?
   c. How often are they conducted?

AGREEMENTS

1. Is there a SOFA for this port?

2. Are there MOU/MOA?

3. If any of the above, are there any limitations on security operations by U. S. forces?

ENCLOSURE 2 TO TAB B TO APPENDIX 6 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
AIRFIELD CHECKLIST (U)

USNORTHCOM AIRFIELD SECURITY ASSESSMENT CHECKLIST FOR IN-TRANSIT AIRCRAFT

When conducting an airfield survey, the questions in this sample Airfield Security Assessment Checklist should be answered and included in the overall survey report. This checklist should be used in conjunction with the guidance in Tab B to Appendix 6 to Annex C of the USNORTHCOM AT OPORD.

1. (U) The paragraph format and numbering in the sample below should be adhered to.

2. (U) When on-site multi-disciplined assessment teams are required for Security CAT "B" airfields teams will complete all items on this checklist. The airfield assessment team chief will ensure the report is forwarded electronically to the responsible DoD Element for inclusion in the airfield portion of the USNORTHCOM Joint Risk Assessment Management Program (JRAMP) database.

3. (U) When on-site multi-disciplined assessment teams are not required for Security CAT 2 airfields, the checklist and survey report may be completed by aircrew members, or security personnel accompanying the aircraft, Individual(s) conducting the survey/ assessment will forward the report electronically to the responsible DoD Element command.

4. (U) For Security CAT 1 airfield assessments and other items determined to be critical by the responsible DoD Element will be completed by aircrew members or others as deemed appropriate.

5. (U) The Airfield Security Assessment Checklist and accompanying information must be marked, handled and stored, at a minimum, as For Official Use Only (FOUO)/Sensitive But Unclassified (SBU). When all items in the checklist are completed and associated with an AT Plan or specific mission, the classification of the document in its entirety will be CONFIDENTIAL, although extracted data may remain FOUO/SBU.

SAMPLE AIRFIELD SECURITY ASSESSMENT CHECKLIST

Airfield Name/Location (Country):_____
ICAO:_____
Date(s) Assessment Conducted: _____
Organization Conducting Assessment:_____
Assessment Team Point of Contact (POC):_____
POC Contact Information (Tel/Fax/Email):_____

(NOTE: International Civilian Aviation Organization [ICAO] codes may not be available for all airfields. ICAO codes can be found in the airfield RAMP for previously assessed airfields.)

SECTION I: PHYSICAL SECURITY.

1. Fencing/Walls.

a. Is the airfield perimeter completely fenced or walled (type, height, condition, gaps, holes, etc.)?

b. Is the flight line/ramp fenced? Describe (type, height, condition, gaps, holes, etc.).

c. Are there clear zones on each side of the fence/wall? If so, describe the clear zone to include width and nature.

d. Is the airfield perimeter or flight line area posted “No Trespassing” or “No Admittance”?

e. Other Physical Barriers.

(1) List different types, locations and numbers of barriers used on the perimeter and on/near the flight line/ramp.

(2) Is the airfield or aircraft parking areas under surveillance, e.g., Closed Circuit Television (CCTV)?

2. Security Force Level.

a. How many guards are typically on duty during the day and night?

b. Are these guards host nation military units? Police or security police? Contract guards?

c. To what extent can the existing security force be augmented by in-place or nearby personnel? How long can the augmented posture be maintained?

d. What are shift durations and shift change procedures/times?

e. What local customs or other factors might result in degraded security, e.g., national holidays, traditional daily rest periods, etc.?

3. Security Personnel.

a. Are personnel well trained and professional? Does this vary by position? Are the supervisory personnel better trained or more motivated?

b. What factors may make individual members or groups susceptible to blackmail or bribery, e.g., low pay, irregular pay, and mistreatment by senior leadership, etc.?

c. Is the reliability of the security guard force in question?

d. What is the predominant language or dialect spoken by security forces? Indicate what percentage of the security force speaks English (if applicable)?

e. To what degree are they willing to work with DoD personnel?

f. Are security forces willing and able to provide increased security?

(1) If so, how are such arrangements made? Through local/State/federal agencies?

4. Security Patrols.

a. Is the perimeter and/or flight line controlled by armed guards?

b. What is the frequency and regularity of patrols? Are the patrols conducted on a predictable schedule, or are they conducted randomly by the airfield security force? If they are not conducted on a regular schedule, is the variance purposeful, e.g., a security measure?

c. Are patrols made on foot, animals, or vehicles?

d. How many people are on each patrol?

e. Do patrols use working dogs?

5. Security Equipment.

a. Are guards armed?

(1) What types of weapons are carried by guards?

(2) Do guards have adequate ammunition levels? What is the basic load?

b. What additional weapons are available (what weapons can be used, if needed; what weapons are used on vehicles, at entry points, guard towers, etc.)?

c. What forms of communications gear do the security personnel use?

d. Do the security personnel have protective masks available?

e. Do the security personnel wear body armor/bullet resistant vests/helmets?

f. Are explosives detector dog teams available and employed?

6. Watch Towers/Fixed Guard Positions.

a. How many ground level guard shacks, elevated towers, fixed fighting positions and/or bunkers, etc., are there? List by location and give description.

b. How many guards are there at each location?

7. Quick Reaction/Counterterrorist Units.

a. Does such a force exist?

b. Is it on or near the airfield?

c. What is the reaction time of this force?

d. How large a force is it?

e. What are the command and control arrangements? To what degree is responsibility delegated in crisis situations?

f. How is the force trained and equipped?

g. Does it have higher morale than the regular guard force?

h. Has it successfully conducted operations in the past?

8. Access Control Points (ACP).

a. Is entry to the installation and flight line/ramp controlled?

b. How many ECPs are there on the perimeter and flight line/ramp areas? Give the location and description of each ECP.

c. Are gates locked if unmanned?

(1) Describe the type of gate (and locking device, if applicable).

d. How many guards are there at each ECP (include type: military, police, or contract guards)? Do numbers vary between day and night operations? If so, describe.

(1) Are interior ramp access doors locked or have controlled entry when open?

e. Are X-ray machines and/or metal detectors used at any of the entry points?

f. If entry is controlled, what form of personal identification is required for individuals and vehicles? Distinguish between airfield and flight line/ramp procedures.

g. Are private vehicles allowed on the flight line/ramp? If so, what method of registration (or pass system) is required?

h. Are all persons in a vehicle required to show identification?

i. What are the visitor control procedures, e.g., procedures for visitor approval, and identification of same?

j. What are visitor escort procedures?

k. To what degree are vehicles, personnel, and their possessions searched?

l. Do any of the above procedures vary at night, e.g., all personnel must show identification at night when entering the installation, airfield or flight line/ramp, etc.?

9. Lighting.

a. Is the entire boundary of the airfield, flight line, and/or aircraft parking ramp lighted at night?

b. Are additional fixed spotlights located at watchtowers and/or entry points?

c. Are mobile mounted/towable spotlights available?

10. Parking.

a. Are DoD aircraft parked in special locations (isolated from other aircraft)? If so, are additional guards posted?

(1) What is the distance from buildings, perimeter fence and non-DoD aircraft?

(2) Are barriers available for aircraft parking locations?

b. Is the area clearly marked as a restricted and/or controlled area?

c. Are DoD personnel authorized to have weapons on the flight line/ramp?

d. Are Service approved weapons storage facilities available to transiting crews?

11. Billeting. Complete the following when it is anticipated that DoD aircraft may be required to remain over night at non-military airfields.

a. Is there billeting nearby? If billeting is unavailable near the airfield, is there a list of hotels that meet minimum security requirements?

b. If there is a list of recommended hotels, request the following information on each, if available:

(1) Basic description (design, height, interior/exterior entrances, number of rooms).

(2) General layout (parking areas, fencing, lighting, proximity to highways and/or major roads).

(3) Number of elevators/stairways (internal/external), building entrances/exits, security features for rooms, vehicle entrances/exits.

(4) Are DoD personnel billeted in the same areas of the hotel, or are they separated? Are there telephones in the rooms?

(5) How is the crew transported to and from the hotel?

(6) Are metal detectors/x-ray machines used at hotel entrances?

(7) Is there a 24-hour front desk operation?

(8) Is there a 24 hour armed hotel guard force?

(9) Are security forces available to escort crews transiting to/from the airfield?

12. Off Installation Route Security. Complete the following when it is anticipated that DoD aircraft may be required to remain over night at non-military airfields.

a. What is the distance from airfield to hotel?

b. How many different routes are there from airport to hotel?

(1) Provide a description of each route.

(2) Identify choke points on each route to include excessive traffic lights and congestion points. Note the location of any bridges, overpasses or tunnels along the route.

(3) Identify number of lanes each way.

(4) Identify one-way streets.

(5) Identify the number and location of safe houses (i.e., police stations) along each route.

c. Do host nation security authorities regularly patrol these routes?

(1) Are host nation security escorts available?

d. Has there been any reported incidents of surveillance in the past 12 months?

13. Physical Location.

a. What natural and/or manmade obstacles are in the vicinity of the airfield, e.g., power lines, tall buildings, etc.?

b. Are there areas surrounding flight line parking area that could be used by hostile elements to covertly observe airport operations and to launch attacks?

c. How suitable is the surrounding terrain and vegetation for staging a stand-off attack? Does this vary seasonally?

d. What is the proximity of vehicle parking and public access areas to the aircraft parking area?

e. Are there high-speed avenues of approach to the aircraft parking area?

14. Maps. Include maps of the local area and/or sketches identifying security related information (e.g., aircraft parking areas, fencing, lighting, ECPs, etc.). Digital photos of all key features are requested, if capability exists and when acquiring such photography is permitted by local authorities.

15. Other items of interest not covered in the checklist.

SECTION II: AIRFIELD SERVICE PROVIDERS CHECKLIST (Fuel, In-Flight Food, Baggage Handling, Janitorial, etc.)

16. Description of facility/service surveyed:

17. Individual(s) interviewed:

a. Name, Rank/Grade, Organization, Phone Number.

18. Service Vendor Control.

a. For each Service Provider, determine:

(1) Contractor Name (if different from Interviewee listed above):

(2) Supervisor's Name:

(3) How long has the service been supplied?

(4) Is there an up-to-date list of names and addresses of all contractor employees?

(a) Are background checks accomplished on the contractor and subcontractor employees? Is a favorable background check required for employment?

1) Are the background checks available for review?

(5) Do vehicles of contractor employees, which enter the facility, have an identifying decal (or pass system)?

(6) Are the vehicles of contractor employees inspected?

(a) How Often?

(7) Is there an identification system for contractor employees?

(a) Are picture identification badges used?

b. How are vendors controlled on the flight line/ramp?

c. Is a single egress/ingress control point to the flight line/ramp used for all vendors, repairmen, etc.?

19. Vendor Vehicle/Equipment Security.

a. Are the vehicles/equipment marked with vendor logo(s)?

b. Are key control procedures used by the vendor?

(1) Who is responsible for issuance of keys?

(2) Are all keys accounted for?

(3) Is issuance of keys recorded?

(a) Are keys signed for?

(b) Is report kept up to date?

(4) Who has access to Master keys? (Name, Position, Number of people)

(5) Are keys removed from vehicles when not in use, at night and on weekends?

(6) Is there a procedure for return of keys when an employee is terminated or transferred?

(7) Physical vehicle/equipment control

(a) Is there a designated parking area for service vehicles on or near the flight line? What is the approximate size and location of the area? Is it fenced off?

1) Is the area in view of assigned personnel during normal working hours?

20. Vendor Service Capability.

a. For each service provider, determine the following:

(1) On average, how many vehicles/pieces of equipment are in service?

(2) What is the average response time?

SECTION III: HOST NATION MEDICAL FACILITIES

21. Hospital Information.

a. Location, phone numbers, POCs

b. What is the distance from the airfield (time by air/ground)?

c. What type of hospital (Military/Civilian)?

d. Does Support Agreement or MOU exist with the hospital?

22. Services Available.

a. What is the inpatient capability and number of beds?

b. How many ICU beds are there?

c. What is the Emergency Service Capability?

(1) What resources are available?

(2) What is the size and experience of the staff?

d. Is there an Emergency Medical Response capability?

e. Is there a HAZMAT/NBC Response capability?

f. Is equipment such as X-ray, CT Scan, MRI available (condition of equipment, availability of support equipment, quality of images)?

g. Are Lab facilities available (capabilities, condition of facilities)?

h. How many ambulances are available? What is their capacity?

i. Is there a Blood Bank? How many Units are available?

j. Is there a Burn Center?

k. Are there Decontamination/Isolation Areas?

23. Medical Evacuation.

a. Are there existing airstrips capable of supporting aircraft used for evacuation?

b. Does a rotary wing evacuation pad exist?

c. Does the host military operate an aeromedical evacuation system already, and will this system be available to U.S. forces? List contacts and telephone numbers.

d. Is liquid or gaseous oxygen available?

e. Do the host civilian authorities operate an aeromedical evacuation system already, and will this system be available to U.S. forces? List contacts and telephone numbers.

f. How would U.S. personnel request medical support and evacuation (including local ground evacuation)? What procedures should be expected for evacuation?

24. Lodging, Food, & Water.

a. What are the lodging provisions for aircrews? (See items 11-13, above)

b. Is there a sanitary Linen/Room/Environment?

c. Is the water and plumbing acceptable (sink/toilet)?

d. If malaria is of concern, are there screens on windows or functioning air conditioning?

e. What are the arrangements for feeding aircrews? (e.g., distance from airfield, same as lodging, etc.)

f. Have off-base food facilities been inspected by host nation civilian or military Preventive Medicine personnel? List POC and telephone numbers.

(1) Are inspection reports available? Obtain copies.

g. What is the source of meat products?

h. What is the source of frozen products?

i. What is the source of dry goods?

j. What is the source of fresh products?

k. What is the source of dairy products?

l. Are adequate food storage facilities available for dry items?

m. Are adequate food storage facilities available for refrigerated/frozen items?

n. Are food-handlers (cooks and servers) aware of HACCP-type guidelines?

o. Does facility appear sanitary (absence of rodents, clean food contact surfaces, etc.)?

p. Are approved food sources, including bottled water, available?

q. Are local sources for bottled water products available? List what to avoid if any.

25. Public Water System.

a. Does a public water system exist?

b. If yes, is it owned/operated by military or civilian authorities? (If possible, obtain POC and telephone numbers.)

c. What is the source of water, e.g., groundwater, surface water or groundwater under the influence of surface water?

d. Will time allow further assessment as to whether the water can be used for potable and/or non-potable purposes? Note: water produced by existing facilities should be considered unsafe until evaluated by preventive medicine personnel.

e. Is there an active drinking water surveillance program from the host nation?

f. What is the form of treatment, disinfection, water quality sampling (collection, analysis, etc.)?

g. Based on host nation laws and regulations, what parameters are analyzed and at what frequencies?

26. Environmental/Industrial.

a. What are the Temperature/Climate/Humidity parameters ("time of year" conditions which would effect disease transmission + assessment of climate factors which would modify current transmission potential)?

b. How is disease transmission affected by the environment (vectors, flora, fauna, etc. Note source of information, e.g., observed vs. documented)?

c. What pollution exists (type, source, concerns, etc.)?

d. Are roads in good repair, streetlights, pedestrians, sidewalks, curbs, etc.?

e. Does environmental pollution appear to be a potential problem?

f. If yes, would it appear to be a threat to DoD personnel?

g. Do potential environmental/pollution hazards exist and in what form (nuclear power plant, fuel storage, chemical plants, agricultural spraying)?

h. Do Hazardous Material/Hazardous Waste (HM/HW) storage, handling, disposal practices exist?

(1) If yes, would they appear to be a threat to DoD personnel?

(2) If yes, supply additional information (type hazard, description, specific location, etc.).

(3) Does the site (airfield and billeting) have the capability to respond to HM/HW release to the environment, e.g., chemical spills?

SECTION IV: HOST NATION FIRE DEPARTMENT

27. Fire Department general information

a. Does the airfield have a fire department?

b. Is the fire department a 24-hour operation?

(1) If not, what are the operating hours?

c. Is the fire department located near the flight line? Do they have quick access to the flight line?

d. What equipment does the fire department have?

(1) Is equipment operational?

e. Are the fire department personnel trained?

f. How do DoD personnel request fire department response?

ENCLOSURE 3 TO TAB B TO APPENDIX 6 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
IN-TRANSIT CHECKLIST (U)

SECURITY ASSESSMENT CHECKLIST FOR IN-TRANSIT GROUND FORCES

The following checklist is designed to assist planners when conducting security assessments of departure points, routes, and arrival points for ground forces in-transit. This checklist should be used in conjunction with the guidance in Appendix 6, Tab B. When completed, the information should be marked, as a minimum, "FOR OFFICIAL USE ONLY".

Assessment and Security Planning Considerations	**Remarks**
What is the DIA/USNORTHCOM Terrorism Threat Level in the AOR?	
Identify what terrorist threats exist, and if they have popular support.	
What are the most likely threat models/scenarios, in the absence of a known threat?	
What other types of threats, such as Para-military organizations or hostile intelligence, could target the operation?	
What is the pre-disposition of local populace to Americans and the presence of the U.S. military forces?	
How could the operations be affected by civil disturbances protesting U.S. policy?	
What are the patterns or incidents attributed to the various threat?	
Identify criminal threats that could affect the unit’s deployment.	
Identify criminal threats that could impact on friendly operations (vandalism, gangs, organized crime, drugs etc).	
Identify all off-limit areas or sections of the AOR that personnel should avoid due to criminal or terrorist threat.	

Conduct threat and vulnerability assessments of all routes and planned halts prior to movement.	
What vulnerabilities must be minimized in order to defeat the threat(s) in the AOR?	
Identify critical routes routinely used by soldiers while traveling through high threat areas.	
Identify critical points along each route and the likely danger posed at each point.	
What facilities will the deployed force occupy or assume responsibility for securing (tent city vs. hard site) (urban or rural location)?	
What type of facilities are available for AA&E, classified, high dollar and sensitive items (motor pool, warehouse, arms rooms etc)? Are the facilities secured?	
Identify potential high-speed avenues of approach.	
If the unit is co-located with local or friendly forces, what are the security responsibilities for those elements?	
If the unit has any High Risk Personnel (HRP) assigned, who approves the designation or level 1 or 2 HRP in the unit AOR?	
What is the nomination and approval process for HRP in the AOR? Are nominated personnel in need of personal protection identified and designated?	
What security measures can be made available to designated HRP?	
What Host Nation support is available to provide HRP protection (on/off post)?	
Who will be responsible to coordinating for protection of HRP (on/off post)?	
Were HRP protective measures based on assessment threats and personal security vulnerabilities?	
What is the AOR Traffic Control and Circulation Control Plan, and what movement restrictions are required and must be enforced?	

What MP assets are available in the AOR, and how does the unit obtain law enforcement support?	
How the unit will obtain assistance from local police liaison, if required?	
Which unit will be designated to augment the military police force in AOR contingency plans?	
What type of initial response and augmentation security forces are in place (local/State/federal, U.S. contractor, military, police)?	
Who is responsible for C2 for FP, if the task force occupies facilities with Host Nation or friendly forces?	
How reliable and well trained are local, State and Federal forces?	
What are the AOR ROE and guidance on the use of deadly force?	
Do AOR ROE match the ROE training given to soldiers prior to deployment?	
With whom will the unit coordinate concerning force protection (Host Nation, friendly force)? What are the capabilities and responsibilities of friendly forces (Allies, Host Nation armed forces, police and security forces, etc.) in force protection operations?	
Do FPCON measures in the AOR need to be modified or supplemented? What are the unit responsibilities under each FPCON?	
What emergency services (fire, medical, bomb detection/disposal, SRT) are available to support the unit's plans, and how is emergency notification conducted?	
What type of services will be provided by friendly forces, or the Host Nation? Are these agencies properly equipped?	
What facilities are identified and will be available to support mass casualties? How will casualties be evacuated?	
What type of communications support is available?	

Are there unique reporting requirements that support the AOR intelligence collection and dissemination programs?	
What procedures the unit must follow to ensure that information system are not compromised?	
What security measures will be implemented at unit level in order to comply with the AOR physical security programs requirements (arms rooms, AA&E, sensitive items, COMSEC)? Who will coordinate with the MP?	
What special contingency plans are needed for the AOR, and how will they impact the unit (mass casualty, bomb threats, alarms and alerts, WMD, terrorist attack, civil disturbances)?	
Annex A: Security Plan	**Remarks**
Identify the EEFI and CCIR that deployed units must protect or collect.	
Use the results of the assessment to develop security plans for self-protection while in transit.	
Determine the appropriate FPCON and establish locally tailored, mission specific measures and standards.	
Identify the requirements for security augmentation, tailored intelligence/ counterintelligence support, host nation assistance and planned alternate routes.	
Ensure the security plan for movement to or through high threat areas is approved by higher HQ.	
Ensure security measures adequately address vulnerabilities and identify the responsibility of the commander or senior representative who will accompany the movement.	
Ensure the plan provides specific guidance on planning and coordinating maintenance recovery and evacuation procedures.	
Ensure the plan provides specific guidance on planning and coordinating medical evacuation procedures.	
Ensure the unit has a movement tracking system in place to provide oversight for high-risk movements	

Ensure the plan addresses maintaining secure communication between moving units and the operations center directing response force operations.	
Ensure the plan addresses how to execute appropriate security measures during rest stops.	
Ensure the plan varies routes and times to break patterns and create uncertainty.	
Update VAs prior to each movement.	
Incorporate a Random Antiterrorism Measures Program (RAMP) into the security plan.	
Determine if the plans effectively cover base security, movement security and security during operations.	
Determine how often the plan will be tested and how the unit should respond.	
Determine how the unit will prepare and test its role in RAMP and FPCON implementation. Are adequate materials on hand?	
Determine what type of contingency plans need to be established to help minimize threat within the AOR (bomb threat plan, fire response plan, Hazmat).	
Determine what type of perimeter, barriers, lighting and access control measures are required when considering the threat/METT-TC (Mission, enemy, terrain, troops, time, civilians).	
Determine which checkpoints and barriers are necessary to control compound access and ensure adequate standoff.	
Determine where will mission essential vulnerable areas (MEVA) be established. Identify their vulnerability to attacks or observations.	
Pre-Deployment Training and Exercises Must Include:	**Remarks**
Completion of Level I AT training or refresher training within the past year for all personnel.	
Completion of Level II AT training for each battalion, separate company, squadron, or ship AT Officer.	

Individual and collective training on all tasks supporting security measures contained in the security plan.	
Performance-oriented training that uses vignettes and AT scenarios for realistic and challenging training.	
Training on rules of engagement for all countries or areas the force will transit or occupy.	
ROE training that requires forces to apply the rules of engagement in various scenarios they are likely to encounter.	
Comprehensive country or area threat briefs.	
Training on weapons and equipment forces may use in the execution of planned security measures.	
Exercises that require transition to higher Force Protection Conditions and incident response.	
Exercises that require reporting procedures and incident response.	
What additional AT awareness or training requirements must be accomplished before/after arriving in the AOR.	
Who is responsible for conducting the training and what records are required.	

TAB A TO APPENDIX 7 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
IPL AND POM DATA SUBMISSION TEMPLATE (U)

Fill out the following template. Each section must be accomplished. Be sure to check classification/portion markings once completed.

1. (U) Title of critical issue/problem area (title must be unclassified):

2. (U) USNORTHCOM Critical Capability: Integrated Force Protection

3. (U) Point of Contact for this submission:
   (U) Name:
   SIPRNet E-Mail:
   Unclassified E-Mail:
   DSN telephone:
   Commercial telephone:
   Fax:

4. (U) Concise statement of how the critical issue/problem would impede USNORTHCOM's ability to achieve its mission objective(s):

a. (*Classification*) Describe the issue/problem in strategic and operational terms.

b. (*Classification*) Explain the mission impact(s) in terms of strategic and operational effects if the issue/problem is not resolved.

c. (*Classification*) Describe what specific non-material solutions you have pursued to rectify the issue/problem (doctrine, organization, training, etc.).

5. (U) Current and recommended program and budget for the issue/problem:

($K) Program Name (PE xxxxxx)	FYxx (current year)	FYxx	FYxx	FYxx	FYxx	FYxx	FYxx
Baseline	XX.X	XX.X	XX.X	XX.X	XX.X	XX.X	XX.X
Proposed Enhancement	XX.X	XX.X	XX.X	XX.X	XX.X	XX.X	XX.X

Figure C-7-A-1

a. (U) Program Description: (what exactly does the baseline program funding buy?)

b. (U) Enhancement Description: (what exactly does the proposed additional funding buy -- list specific items/commodities and costs):

6. (U) Primary *and* alternate agents responsible for the recommended solution (is this program executed by HQ USNORTHCOM, or by a Service, or by a Defense Agency?):

HQ USNORTHCOM	___Pri ___Alt
Army / FORSCOM	___Pri ___Alt
Navy / CFFC	___Pri ___Alt
AF / ACC	___Pri ___Alt
Marines / MARFORNORTH	___Pri ___Alt
Agency (*specify*)	___Pri ___Alt
Other (*specify*)	___Pri ___Alt

7. (U) Rationale for why the agent(s) indicated above are responsible for the recommended solution:

8. (U) Linkages:

a. (U) Does your issue/problem link to the current UCP? Y / N
If yes, explain and cite reference page(s):

b. (U) Does your issue/problem link to the Strategic Planning Guidance? Y / N
If yes, explain and cite reference page(s):

c. (U) Does your issue/problem link to the Joint Planning Guidance? Y / N
If yes, explain and cite reference page(s):

d. (U) Does your issue/problem link to the Contingency Planning Guidance? Y / N
If yes, explain and cite reference page(s):

e. (U) Does your issue/problem link to USNORTHCOM CONPLAN(s)? Y / N
If yes, explain and cite plan(s) and reference page(s):

f. (U) Does your issue/problem link to another combatant command's CONPLAN or OPLAN for which USNORTHCOM owns a supporting plan? Y / N
If yes, explain and cite plan(s) and reference page(s):

g. (U) Does your issue/problem link to a DoD or Joint directive? Y / N
If yes, explain and cite the directive and reference page(s):

h. (U) Was your issue/problem included in a prior USNORTHCOM IPL? Y / N
If yes, explain and cite reference page(s):

i. (U) Did the primary agent identified in item 5. above include the issue/problem in its most recent POM? Y / N
If yes, explain and provide name, organization, phone #, and email contact info of Program Manager/Analyst:

j. (U) Was your issue/problem identified in a Joint Quarterly Readiness Review (JQRR)? Y / N
If yes, explain and cite JQRR number and reference page(s):

k. (U) Is your issue/problem assigned to and being worked by a Joint Staff Functional Capability Board? Y / N
If yes, identify which FCB, explain actions to date and status of the issue within the FCB process, and provide name, organization, phone #, and email contact info of FCB Analyst:

9. (U) Additional Information: Provide any other information you deem pertinent to the issue/problem that will help USNORTHCOM J34 and J8 resolve the issue/problem.

TAB A TO APPENDIX 8 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
SAMPLE REQUEST FOR DEVIATION (U)

1. (U) N-NC/J4 is coordinating with NC/J34, OSD and the SEWG to develop specific AT construction deviation request procedures for the USNORTHCOM AOR. In the interim, the DoD Elements will, IAW UFC 4-010-01, paragraph 1-1.2.3, continue to utilize Service and Agency/Field Activity-specific AT construction and deviation request processes. DoD Elements will submit AT construction deviation requests through their chains of command to OSD and will provide copies of deviation requests to USNORTHCOM for the following structures: billeting, primary gathering buildings, and *Critical Facilities (ref UFC 4-010-01, paragraph 1-5.3). N-NC/J4 will consolidate these requests into an annual report to Commander, USNORTHCOM NLT 30 September of the current Fiscal Year (FY). Commander, USNORTHCOM retains the right to review and make change recommendations to OSD on these deviation requests. *(*Critical Facilities is defined by UFC 4-010-01, paragraph 1-5.3 as: Buildings that must remain mission operational during periods of national crisis and / or if subjected to terrorist attack should be designed to significantly higher levels of protection than those provided by these standards.)*

2. (U) USNORTHCOM is the approval authority for all deviations from USNORTHCOM-directed AT requirements to include AT Design Standards contained in Appendix 8 to Annex C. USNORTHCOM cannot approve deviations from DoD AT requirements to include DoD construction standards. Such deviation requests must be submitted through USNORTHCOM to the Joint Staff for consideration and action.

3. (U) A deviation request is not required for standoff requirements, if equivalent protection (hardening of the structure) is provided. In other words, if the required stand-off distance cannot be obtained but the structure is hardened to provide an equal level of protection against a baseline weapon, then no deviation has occurred.

4. (U) The information areas on the sample deviation request form should, when properly filled out, provide approval authorities with sufficient details to reach a decision.

5. (U) Instructions for completing selected items:

a. (U) Item 4: Include information on each deviation if multiple deviation approvals are required.

b. (U) NOTE: Submit one request for each facility, building, or unique set of circumstances.

SAMPLE REQUEST FOR DEVIATION FROM CONSTRUCTION STANDARDS

FROM: Originating Unit/Agency

THRU:

TO:
HQ USNORTHCOM/J34 or Service/Combatant Command/Agency/Field Activity Headquarters
250 Vandenberg Street, Ste B106
Peterson AFB, CO 80914-3817

1. TYPE OF REQUEST

☐ CONSTRUCTION STANDARD/STAND-OFF ☐ PROCEDURAL

☐ FPCON MEASURES ☐ OTHER

2. TYPE OF DEVIATION

☐ EXCEPTION (Permanent) ☐ TEMPORARY DEVIATION (Waiver) ☐ TECHNICAL DEVIATION (Variance)

ITEM 3 – AFFECTED BUILDING, INSTALLATION OR ORGANIZATION/UNIT (Including building number, type of facility, and installation or location. Include street address and city for off-installation facilities). Do not abbreviate.

3.

ITEM 4 – SPECIFIC REQUIREMENT (S) FOR WHICH DEVIATION IS REQUESTED (Reference and Text)

4.

ITEM 5 – NUMBER OF PERSONNEL WHO OCCUPY THE SPECIFIED BUILDING OR INSTALLATION DURING ROUTINE OCCUPANCY, AT ANTICIPATED PEAK OCCUPANCY, AND AT MAXIMUM OCCUPANCY.

5. NORMAL OCCUPANCY =
ANTICIPATED PEAK OCCUPANCY =
MAXIMUM OCCUPANCY =

ITEM 6 – IF DEVIATION IS REQUESTED FROM A CONSTRUCTION STANDARD OR STANDOFF REQUIREMENT, PROVIDE COST OF:
A. PLANNED DESIGN /RENOVATION.
B. DESIGNED MODIFICATION TO PROVIDE UFC MANDATED LEVEL OF PROTECTION AT AVAILABLE STAND-OFF BASED UPON UFC THREAT WEAPON/IED.
C. DESIGNED MODIFICATION TO PROVIDE UFC MANDATED LEVEL OF PROTECTION AT AVAILABLE STAND-OFF BASED UPON USECUOM THREAT IED.

6. A. $
   B. $
   C. $

ITEM 7 – INDICATE WHY THE COSTS IN ITEM 6.B. AND 6.C. ARE PROHIBITIVE OR CONSIDERED EXCESSIVE.

7.

ITEM 8 – IF DEVIATION IS REQUESTED FOR A CONSTRUCTION STANDARD, PROVIDE AS AN ATTACHMENT AN ENGINEER ANALYSIS TO SUPPORT MITIGATING MEASURES IN PLACE OR PLANNED IN LIEU OF COMPLIANCE WITH THE EXISTING STANDARD, ITS COST, AND ESTIMATED COMPLETION DATE.

8.

ITEM 9 – INDICATE EXTENT OF RELIEF REQUESTED AND, IF A WAIVER IS REQUESTED, THE REQUESTED TIME PERIOD. FOR LEASES, INDICATE PLANNED YEARS OR MONTHS, NOT "DURATION OF THE LEASE".

9.

ITEM 10 – PROVIDE A RISK ANALYSIS STATEMENT OR ATTACHMENT FOR THE DEVIATION, IF ANY, ON THE SAFETY OF U.S. FORCES OVER THE REQUESTED DEVIATION PERIOD.

10.

ITEM 11 – PROVIDE A JUSTIFICATION FOR THE DEVIATION, AND IF A PERMANENT DEVIATION IS REQUESTED, EXPLAIN WHY A TEMPORARY DEVIATION WOULD NOT BE SUFFICIENT

11.

ITEM 12 – INDICATE COMPENSATORY MEASURES PLANNED OR CURRENTLY IN EFFECT. IF PLANNED, INCLUDE ANTICIPATED START DATE.

12.

ITEM 13 – PROVIDE PROPOSED LONG TERM CORRECTIVE ACTION (IF APPLICABLE)

13.

ITEM 14 – INDICATE IF COMPLIANCE REQUIRES HOST NATION ACTION OR APPROVAL AND HAS BEEN APPROVED. PROVIDE SUMMARY OF REQUEST AND RESPONSE.

14.

ITEM 15 – IMPACT STATEMENT (WHAT IS THE IMPACT ON THE ORGANIZATION OR MISSION IF TH DEVIATION REQUEST IS DISAPPROVED?)

15.

ITEM 16 – COMMENTS / REMARKS

16.

17. SUBMITTING UNIT POINT OF CONTACT
RANK / NAME:
TITLE:
PHONE / FAX:
E-MAIL:

ENCLOSURES:
Scaled installation maps or diagrams showing subject locations are requested for construction / standoff deviation requests. (Drawings or photographs are requested if they will assist the approval authority in evaluating the request.)

SUBMITTING COMMANDER OR OFFICIAL DATE

Signature
SIGNATURE BLOCK

REVIEWING OFFICIAL (Component) DATE

RECOMMENDATION

☐ APPROVAL ☐ DISAPPROVAL ☐ OTHER

COMMENTS:

PHONE / FAX:
E-MAIL:

Signature
SIGNATURE BLOCK

USNORTHCOM APPROVAL OR CONCURRENCE AUTHORITY DATE

☐ APPROVED/CONCUR ☐ DISAPPROVED ☐ OTHER

COMMENTS: (IF TEMPORARY DEVIATION, INCLUDE TERMINATION DATE)

DISTRIBUTION:

1 - REQUESTING UNIT
2 - APPROVAL AUTHORITY

CLASSIFIED BY – OR – DERIVED FROM:
REASON: (not required for derivative classifications)
DECLAS:

TAB B TO APPENDIX 8 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
CHECKLIST FOR USE IN CONTRACTING SUPPORT (U)

1. (U) What is the specific support service or product required? Define the exact requirement. Have alternatives to contracting for the service or support been identified? Have alternative sites been considered?

2. (U) Is there a current Threat/VA for the country/location? When was it last performed? What is the identified threat? What are the vulnerabilities?

3. (U) What is the level of security provided at the location? Are there extra security measures employed as a result of a VA or CI report that mandates extra AT measures?

4. (U) What are the capabilities for security and AT measures?

5. (U) What additional security measures can the Contractor provide during the deployment, stop or exercise for service and support? What specifically can the Contractor do to augment the existing security arrangements and the U.S. military?

6. (U) Can the contractor properly vet the security clearance for all employees involved in supporting the U.S. force bed-down site/ship/aircraft? What measures of uncertainty still exist after vetting the Contractor employees?

7. (U) Has the force considered asking for periods of support or service that are not routine or predictable to reduce risk of exposure? How can the coordination with contractor ensure a more unpredictable time period of coverage?

8. (U) If the contractor is unable to provide extra OPSEC or AT measures, can military provide extra assistance? Can the U.S. force add extra AT measures that are vetted with the civilian authorities and approved?

9. (U) Where vetting cannot be achieved or additional AT measures cannot be contracted, what specific AT measures can the force implement to reduce the operational risk?

10. (U) Is the reason for the service or support requirement really needed? Does the operational benefit of receiving the service or support outweigh the security shortfalls identified? Are the support tasks mandated or can operational flexibility be employed to mitigate the overall risk (i.e. can we sail longer before refueling at sea or at some other port facility within the USNORTHCOM AOR which poses a lower risk?)?

11. (U) Have we performed an overall mission analysis of the operation to identify known constraints and restraints?

12. (U) Has the force established a hierarchy of support to satisfy the operational requirements? (i.e. Refuel underway, mil-to-mil, contractor)

13. (U) For Husbanding Contracts, has the force incorporated the following AT considerations, if needed into the contract to ensure the Contractor will:

a. (U) Conduct background checks of all contractor/subcontractor employees.

b. (U) Establish a process for positively identifying all contractor/sub-contractor employees and consider the use of photo IDs, official IDs, U.S. Government-Issued IDs (only after background checks), or company issued IDs as last resort.

c. (U) Limit vehicle access.

d. (U) Provide daily personnel assess list along with photographs to security personnel.

e. (U) Provide daily vehicle access list to security personnel.

f. (U) Identify all watercraft being utilized.

g. (U) Identify all food and water sources being utilized.

h. (U) Move all cars, trash containers at least 75 feet from visiting ships

i. (U) Establish unloading zones a minimum of 400 feet from visiting ships.

14. (U) Have procedures and measures been established to ensure the contractor understands, acknowledges, fully supports and briefs appropriate company and sub-contractor personnel on the AT and security measures to be implemented by the force?

15. (U) Have the following security measures been considered for implementation by the U.S. forces?

a. (U) Physical inspection of all visitors and their suitcases, parcels and other carry-on items.

b. (U) Physical inspection of all vehicles and watercraft.

c. (U) Physical inspection of all buildings and structures within the U.S. controlled exclusion/restricted areas.

d. (U) Conducting aggressive random patrols and spot-checks.

e. (U) Use of military working dogs (MWD) or Explosive Detector Dog Teams (EDDT) to conduct inspections, patrols, and spot-checks.

f. (U) Establishing U.S. controlled exclusion/restricted zone and access control points (ACP).

g. (U) Establishing a security response force for use inside the U.S. controlled exclusion/restricted zone.

h. (U) Use of security equipment: lighting, barriers, night vision devices, electronic security systems, X-ray machines, etc.

i. (U) Considerations for support to aircraft:

(1) (U) Is there a specific threat for aircraft? Is there a specific man portable air defense system (MANPAD) threat? If so, is there a restriction on the use of Aircraft Defense Systems (ADS)? If so, have alternate routes/airfields been considered to reduce the risk?

(2) (U) Is there a restriction regarding the arming of aircraft security teams? If so what are the capabilities of security forces? What are the security procedures at the selected airfields?

j. (U) Considerations for support to strategic sealift fleet:

(1) (U) Is there a specific threat to sealift at sea or in port? Is the crew trained and armed to protect the ship? Is there detection and defense equipment available for the crew's use in protecting the ship?

(2) (U) Are U.S. port handlers included in the AT plan?

(3) (U) Does the sealift have a CBRNE defense capability? Is the crew trained in CBRNE defense?

(4) (U) Have security zones been established? Have picket boats been considered?

APPENDIX 14 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
SAMPLE AT PLAN (U)

1. (U) The format outlined below is offered as one means of developing an AT plan. It is designed for a base or installation, but can be adapted for other facilities and deployed units. It is meant to help the ATO structure the AT plan in a comprehensive and organized manner. The format is patterned after the standard five-paragraph military operations order (Situation- Mission-Execution-Administration and Logistics-Command and Signal). Another available option is to use the Joint Antiterrorism Program Manager's Guide resident within ATEP.

2. (U) This format enables the synchronization of existing programs such as Law Enforcement, Physical Security, AT, OPSEC, INFOSEC, High-Risk Personnel protection and other installation efforts. AT Plans should be integrated into all plans and separate annexes. Remember that staff interaction is a crucial element of developing a realistic, executable plan.

3. (U) Although this sample is patterned after the military operations order, it is applicable to Commanders/Directors of DoD Elements as they develop plans to protect personnel, activities, and material under their control.

4. (U) This sample uses supporting Annexes, Appendices, Tabs, and Enclosures to provide amplifying instructions as required. This method shortens the length of the basic plan (which should be read by all personnel outlined in the plan), and provides organization, structure, and scalability.

INSTALLATION/OPERATION NAME ANTITERRORISM PLAN 2002 (AT-04)

Task Organization. [Include all agencies/personnel (base and civilian) responsible to implement the plan. Include as a separate Annex. See Annex A (Task Organization).]

Maps/Charts: [List all applicable maps or charts. Include enough data to ensure personnel are using the correct year/edition/version of the subject material.]

Time Zone: [Enter the time zone of the installation. Indicate the number of hours to calculate (plus/minus) ZULU time.]

Ref: [Enter the compilation of pertinent publications, references, MOU/MOA/MAA. This list may be included in a separate Annex. See Annex Q (References).]

1. SITUATION.

a. General. [This plan applies to all personnel assigned or attached to the installation. [Describe the political/military environment in sufficient detail for subordinate commanders, staffs, and units to understand their role in the installation AT operations.]

b. Enemy. [The enemy is any adversary capable of threatening the installation's personnel, facilities, and equipment. [ENTER the general threat of terrorism to this installation including the intentions and capabilities, identification, composition, disposition, location, and estimated strengths of hostile forces. Include the general threat of terrorist use of WMD against this installation. This information should remain unclassified when possible. See paragraph 1f, Intelligence, on identifying specific threats.] This information may be included as a separate Annex. See Annex B (Intelligence).]

c. Friendly. [ENTER the forces available (both military and civilian) to respond to a terrorist WMD attack. Include the next higher headquarters and adjacent installations, and any units/organizations that are not under installation command, but may be required to respond to such an incident. These units/organizations may include local, State, or Federal LE agencies and military police forces, fire and emergency services, medical, and federal/State and local agencies, special operations forces, engineers, detection (radiological, nuclear, biological, and chemical) decontamination or smoke units, and explosive ordnance disposal (EOD). Include MOAs/MOUs and any other special arrangements that will improve forces available to support the plan. If in the U.S. and its territories, the Department of Justice, Federal Bureau of Investigation (FBI) is responsible for coordinating all Federal agencies and DoD forces assisting in the resolution of a terrorist incident. If outside the U.S. and its territories, the Department of State (DoS) is the lead agency. This information can be included in a separate Annex(s). See Annex A (Task Organization) and Annex J (Command Relationships).]

d. Attachments/Detachments. [ENTER installation/civilian agencies NOT normally assigned to the installation that are needed to support this plan. Explain interagency relationships and interoperability issues. This can be listed in other Annexes. See Annex A (Task Organization) and Annex J (Command Relationships).]

e. Assumptions. (List planning/execution assumptions) [ENTER all critical assumptions used as a basis for this plan. Assumptions are those factors unlikely to change during the implementation of the AT plan and that must addressed in order to continue to plan. They can range from the installation's troop strength to addressing the local political/social environment. Examples follow:

(1) The installation is vulnerable to theft, pilferage, sabotage, and other threats. The installation is also vulnerable to a WMD attack.

(2) An act of terrorism involving WMD can produce major consequences that will overwhelm almost immediately the capabilities of the installation.

(3) Security personnel, both military and civilian, may be insufficient to provide total protection of all installation resources; therefore, the principal owner or user of a facility, resource, or personnel must develop adequate unit awareness and safeguard measures.

(4) No single unit on the installation possesses the expertise to act unilaterally in response to WMD attacks.

(5) If protective equipment is not available, responders will not put their own lives at risk.

(6) Local, non-military response forces will arrive within [time] of notification.

(7) Units specializing in WMD response will arrive on-site within [number of hours based on installation location] of notification.

(8) The HN is supportive of U.S. policies, and will fulfill surge requirements needed to respond to a WMD incident IAW MOAs/MOUs.]

f. Intelligence. [ENTER the person, staff, or unit responsible for intelligence/counterintelligence collection and dissemination. The installation Commander must have a system in place to access current intelligence. This can be included in Annex B (Intelligence).] [National-level agencies, Combatant Commanders, intelligence and CI systems provide theater or country threat levels and threat assessments. In the U.S. and its territories, local installations must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement, or other Federal agencies.] Obtain these assessments, as they will serve as a baseline for the installation's tailored assessment. The installation should have a process in place for developing the installation's tailored

threat assessment or “local threat picture.” The installation’s tailored threat assessment should be continuously evaluated, updated, and disseminated, as appropriate, and as directed by the installation Commander. The Commander should determine the frequency and the means of dissemination of the installation’s tailored AT product. Note: Commanders cannot change the threat level, which is developed at the national-level although they can declare higher FPCONs than the baseline.

2. MISSION. [ENTER a clear, concise statement of the command’s mission and the AT purpose or goal statement supporting the mission. The primary purpose of the AT plan is to safeguard personnel, property, and resources during normal operations. It is also designed to deter a terrorist threat, enhance security and AT awareness, and to assign AT responsibilities for installation personnel.]

3. EXECUTION.

a. Commander’s Intent. (Commander’s vision on how he/she sees the execution of the unit’s AT Program. Refer to Service planning doctrine for assistance.)

b. Concept of Operations. [ENTER how the overall AT operation should progress. This plan stresses deterrence of terrorist incidents through preventive and response measures common to all combatant commands and Services. During day-to-day operations, the installation should stress continuous AT planning and passive, defensive operations. This paragraph should provide subordinates sufficient guidance to act if contact or communications with the installation chain of command is lost or disrupted.

(1) The installation’s AT Concept of Operations should be phased in relation to pre incident actions and post-incident actions. AT planning and execution requires that staff elements work with a much greater degree of cohesiveness and unity of mission than that required during the conduct of normal base sustainment operations. The AT mission, and the unpredictability of its execution, requires very specific “how to” implementation instructions of DoD FPCON Measures and in what manner these actions must be coordinated. This “how to” element is not normally included in the Concept of Operations paragraph; however the necessity to provide “how to” guidance in the AT plan requires a different manner of data presentation to ensure brevity and clarity. The implementation instructions are put into the form of action sets and can be displayed in the form of an execution matrix (Pre-Incident Action Set Matrix).

(2) In Post-Incident planning, the installation should focus on its response and reconstitution responsibilities upon notification of a terrorist incident and the procedures for obtaining technical assistance/augmentation if the incident exceeds the installation’s organic capabilities. National-level responders (Federal Emergency Management Agency (FEMA), Red Cross, and Federal Bureau of Investigation (FBI)) may not be immediately accessible or available to respond to an installation’s needs. Therefore each installation must plan for the worst-case scenario, by planning its response based on its organic resources and available local support through MOA/MOUs.

(3) The situation may dictate that the installation will not only conduct the initial response but also sustained response operations. Many installations do not have onboard WMD officers or response elements. This paragraph will include specific implementation instructions for all functional areas of responsibility and the manner in which these actions must be coordinated. The implementation instructions can be put in the form of actions sets and displayed in the form of a synchronization matrix (Post-Incident Action Set Synchronization Matrix). The synchronization matrix format clearly describes relationships between activities, units, supporting functions, and key events which must be carefully synchronized to minimize loss of life and to contain the effects of a terrorist incident.

c. Tasks. [ENTER the specific tasks for each subordinate unit or element listed in the Task Organization paragraph. Key members of the installation have responsibilities that are AT and/or WMD specific. The Commander should ensure that a specific individual/unit/element within the installation is responsible for each action identified in this plan. Each individual/unit/element must know the tasks and responsibilities, what these responsibilities entail, and how these will be implemented. While the tasks and responsibilities for each AT planning and response element will be delineated in the Pre- and Post-incident Action Set Matrices, it is recommended that the installation Commander identify/designate the primary lead for each element and enter that information in this paragraph.]

(1) First Subordinate Unit/Element/Tenant.

(a) Task listing.

d. Coordinating Instructions. [This paragraph should include AT specific coordinating instructions and subparagraphs, as the Commander deems appropriate. In addition, this section of the AT plan outlines aspects of the installation's AT posture that require particular attention to guarantee the most effective and efficient implementation of the AT plan. For the purposes of this plan, there are five basic coordinating instructions: 1) AT planning and response elements; 2) Procedural; 3) Security Posture; 4) Threat Specific Responsibilities, and 5) Special Installation Areas. The reader will be directed to specific Annexes that will provide amplifying instructions on these topics. The sections listed below are representative, and may not be all-inclusive.

(1) AT Planning and Response. For instructional purposes, this template outlines AT planning and response elements on the installation required to respond to a terrorist/WMD incident. Initial and sustained response to an attack must be a coordinated effort between the many AT planning and response elements of the installation, based on the installation's organic capabilities. As the situation exceeds the installation's capabilities, it must activate MOAs/MOUs with the local/State/Federal agencies (US and its territories) or HN (outside the U.S. and its territories). For the purposes of this plan, an installation's capability is divided into AT planning and response elements. These tailored, installation-level elements parallel the national-level

FEMA Emergency Support Functions (ESFs) and the JSIVA evaluation criteria to the greatest degree possible.

AT Planning & Response Elements

Information & Planning *
Communications * +
HAZMAT *
Security * +
Explosive Ordnance Disposal (EOD) +
Firefighting * +
Health & Medical Services * +
Resource Support *
Mass Care *
Public Works *
Intelligence Process +
Installation AT Plans/Programs +
Installation Perimeter Access +
Security System technology +
Executive Protection +
Response & Recovery +
Mail Handling +

* Derived from FEMA ESFs
+ Derived from JSIVA assessment criteria

(2) Procedural.

(a) Alert Notification Procedures. See Appendix 14 to Annex C (Operations).

(b) Use of Force/Rules of Engagement. See Annex H (Legal).

(c) Installation Training & Exercises. See Annex N (AT Program Review, Training & Exercises).

(d) Incident Response. See Appendix 1 to Annex C (Operations).

(e) Consequence Management. See Appendix 1 to Annex C (Operations).

(f) High-Risk Personnel Protection Procedures. See Appendix 9 to Annex C (Operations).

(g) AT Program Review (See Annex N (AT Program Review, Training & Exercises).

(h) Higher Headquarters Vulnerability Assessments. See Annex N (AT Program Review, Training & Exercises).

(3) Security Posture Responsibilities.

(a) Law Enforcement. See Appendix 7 to Annex C (Operations).

(b) Physical Security to include Lighting, Barriers, Access Control. See Appendix 6 to Annex C Operations).

(c) Other On-site Security Elements. See Appendix 8 to Annex C (Operations).

(d) Operations Security. See Appendix 10 to Annex C (Operations).

(e) Technology. See Appendix 15 to Annex C (Operations).

(f) EOC Operations. See Appendix 12 to Annex C (Operations).

(g) Critical Systems Continuity of Operations (optional). See Appendix 13 to Annex C (Operations).

(h) Other.

(4) Threat Specific Responsibilities.

(a) Antiterrorism. See Appendix 2 to Annex C (Operations).

(b) Weapons of Mass Destruction. See Appendix 5 to Annex C (Operations).

(c) Special Threat Situations. See Appendix 3 to Annex C (Operations).

(d) Information Security. See Appendix 11 to Annex C (Operations).

(e) Natural/Man-made Hazards (Optional). See Appendix 16 to Annex C (Operations).

(f) Other.

(5) Special Security Areas.

(a) Airfield Security. See Appendix 4 to Annex C (Operations).

(b) Port Security. See Appendix 4 to Annex C (Operations).

(c) Embarkation/Arrival Areas. See Appendix 4 to Annex C (Operations).

(d) Buildings. See Appendix 4 to Annex C (Operations).

(e) Other.

4. ADMINISTRATION AND LOGISTICS. [ENTER the administrative and logistics requirements to support the AT plan, which should include enough information to make clear the basic concept for planned logistics support. Ensure the staff conducts logistical planning for both pre- and post-incident measures addressing the following: locations of consolidated WMD defense equipment; expedient decontamination supplies; Individual Protective Equipment exchange points; special contamination control requirements; retrograde contamination monitoring sites; WMD equipment/supply controlled supply rates and pre-stockage points; and procedures for chemical defense equipment "push" packages. Specific logistics and administrative requirements will emerge throughout the planning process outlined in the Concept of Operations, specifically when developing the action sets. These requirements should be incorporated into this paragraph. Finally, include fiscal instructions on how to support AT operations.

a. Administration. See Annex O (Personnel Services).

b. Logistics. See Annexes D (Logistics) and E (Fiscal).

5. COMMAND AND SIGNAL. [ENTER instructions for command and operation of communications-electronics equipment. Identify the primary and alternate locations of the command post and emergency operations center. Enter the installation's chain of command. Highlight any deviation from that chain of command that must occur as a result of a WMD incident. The chain of command may change based on the deployment of a Joint Task Force or a National Command Authority-directed mission. Identify the location of any technical support elements that could be called upon in the event of a terrorist WMD incident and the means to contact each. Recommend the installation coordinate with higher headquarters to establish procedures to allow for parallel coordination to report a terrorist WMD incident. The installation must provide for prompt dissemination of notifications and alarm signals, and the timely/orderly transmission and receipt of messages between elements involved in and responding to the incident.]

a. Command. See Annex A (Task Organization) and Annex J (Command Relationships).

b. Signal. See Annex K (Communications).

c. Command Post Locations.

(1) Primary: [ENTER location]

(2) Alternate: [ENTER Location]

d. Succession of Command.

(1) First alternate: [ENTER POSITION/TITLE]

(2) Second alternate: [ENTER POSITION/TITLE]

//SIGNATURE//
Commanding General/Officer
Signature Block

ANNEXES: (Should provide amplifying instructions on specific aspects of the plan. Each ANNEX can be subdivided into Appendices, Tabs, and Enclosures as required to provide amplifying instructions. Further, some of these supporting documents may be established in other unit operating orders/procedures, and referenced as required.)

ANNEX A - Task Organization. [ENTER key AT organization composition i.e., AT Working Group, Crisis Management Team, Emergency Operations Center, First Response Elements, etc.]

Appendix 1 – Table of Organization

Appendix 2 – Post Prioritization Chart

ANNEX B – Intelligence. [ENTER the agency(s) responsible for intelligence and specific instructions. In the U.S. and its territories, commanders must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement or other federal agencies]

Appendix 1 – Local Threat Assessment

Appendix 2 – Local WMD Assessment

Appendix 3 – Counterintelligence

Tab A – Counterintelligence Target List
Tab B – Multidiscipline Counterintelligence Threat Report
Tab C – Designation of Theater CI Executive Agency (Draft Message)
Tab D – Umbrella CI Force Protection Source Operation Proposal

Appendix 4 – Risk Assessment

Appendix 5 – Pre-deployment AT Vulnerability Assessment

ANNEX C – Operations. [This is the most important part of the plan]. Annex C and supporting Appendices will provide specific instructions for all the various AT operations. All other Annexes/Appendices support the implementation of Annex C.

Appendix 1 – Incident Planning and Response. [ENTER how the various agencies (military/civilian) and resources will be integrated to respond to the operations outlined below. These instructions should be generic enough to apply across the operational spectrum. Specific instructions for each operation will be detailed in the appropriate Annex/Appendix/Enclosure.]

Tab A – Incident Command and Control Procedures
Tab B – Incident Response Procedures
Tab C – Incident Management Procedures

Appendix 2 – Antiterrorism

Tab A - Mission Essential Vulnerable Assets (MEVA)
Tab B - Potential Terrorist Targets
Tab C – FPCON
Enclosure 1 - FPCON Action Sets. [Who/What/When/Where/How]
Tab D - Random Antiterrorism Measures (RAM) Procedures

Appendix 3 - Special Threat Situations
Tab A - Bomb Threats
Enclosure 1 – Bomb Threat Mitigation
Enclosure 2 – Evacuation Procedures
Enclosure 3 – Search Procedures
Tab B - Hostage Barricaded Suspect
Tab C – Mail Handling Procedures

Appendix 4 – Special Security Areas
Tab A – Airfield Security
Tab B – Port Security
Tab C – Embarkation/Arrival Areas.
Tab D – Buildings

Appendix 5 – Weapons of Mass Destruction (CBRNE) & HAZMAT. [ENTER the specific procedures planning, training, and response to WMD (CBRNE) incidents. Care should be taken to integrate existing plans for response to HAZMAT incidents to avoid duplication. Include “baseline” preparedness.]
Tab A - WMD Action Set Synchronization Matrix [Who/What/Where/When/How]
Tab B – CBRNE Emergency Responder Procedures

Appendix 6 – Physical Security

Tab A – Installation Barrier Plan. [ENTER procedures and pictorial representation of barrier plan.]
Tab B – Installation Curtailment Plan
Tab C – Construction Considerations
Tab D – Facility and Site Evaluation and/or Selection
Tab E – AT Guidance for Off-Installation Housing

Appendix 7 – Law Enforcement
Tab A – Organization, training, equipping of augmentation security forces
Tab B – Alternate Dispatch Location
Tab C – Alternate Arming Point

Appendix 8 – Other On-Site Security Forces

Appendix 9 – High Risk Personnel
Tab A – List of High Risk Billets

Appendix 10 – Operations Security

Appendix 11 – Information Security

Appendix 12 – Emergency Operations Center (EOC) Operations. [ENTER procedure for the activation & operations of the EOC.]
Tab A – EOC Staffing (Partial/Full)
Tab B – EOC Layout
Tab C – EOC Messages & Message Flow
Tab D – EOC Briefing Procedures
Tab E – EOC Situation Boards
Tab F – EOC Security and Access Procedures

Appendix 13 – Critical Systems Continuity of Operations Plans (Optional). [ENTER those systems that are essential to mission execution and infrastructure support of the installation i.e., utilities systems, computer networks, etc. This document outlines how the installation will continue to operate if one or more critical systems are disrupted or fails and how the systems will be restored.]
Tab A – List of installation critical systems
Tab B – Execution checklist for each critical system

Appendix 14 - Emergency Mass Notification Procedures. [ENTER the specific means and procedures for conducting a mass notification. Also covered should be the procedures/means for contacting key personnel and agencies.
Tab A – Situation Based Notification
Tab B – Matrix List of Phone Numbers/Email Accounts

Appendix 15 – Exploit Technology Advances. [ENTER the process and procedures for developing and employing new technology. Identify who is responsible and what should be accomplished.]

Appendix 16 – Higher Headquarters Vulnerability Assessments. [ENTER procedures for conducting higher headquarters vulnerability assessments.

Appendix 17 – Natural/Man-made Hazards (Optional) [Hurricanes, Flooding, Chemical Plants etc.]

Tab A - Locality specific natural and man-made hazards)

ANNEX D – Logistics (Specific logistics instructions on how to support AT operations)

Appendix 1 – Priority of Work. [ENTER the priority of employing scarce logistical resource.]

Appendix 2 – Emergency Supply Services

Appendix 3 – Weapons and Ammunition Supply Services

Appendix 4 – Emergency Equipment Services

Appendix 5 – Evacuation Shelters

Appendix 6 – Generator Refueling Matrix

ANNEX E – Fiscal (Specific fiscal instructions on how to support AT operations from pre-incident through post incident)

Appendix 1 – AT Program Objective Memorandum/Budget Estimate Submission Instruction

Appendix 2 – Combating Terrorism Readiness Submission Instructions

Appendix 3 – Fiscal Management during Exigent Operations

ANNEX F – Tenant Commanders (Specific instructions on how tenant commands/agencies support AT operations)

Appendix 1 – Areas of Responsibility (Pictorial)

ANNEX G – Air Operations (Specific air instructions on how to support AT operations)

Appendix 1 – List of Landing Zones (Used for emergency medical evacuations or equipment/personnel staging areas.)

Appendix 2 – LZ Preparation Procedures

ANNEX H – Legal. [ENTER the jurisdictional limits of the installation's commander and key staff. Although the Department of Justice, Federal Bureau of Investigation (FBI), has primary law enforcement responsibility for terrorist incidents in the United States, the installation Commander is responsible for maintaining law and order on the installation. Once a task force or other than installation support arrives on the installation, the agencies fall under the direct supervision of the local Incident Commander. In all cases, command of military elements remains within military channels. The installation should establish agreements to address the use of other military personnel, and local resources that clearly delineate jurisdictional limits. The agreements will likely evolve into the installation having responsibility "inside the wire or installation perimeter" and the local authorities having responsibility "outside the wire or installation perimeter". There may be exceptions due to the wide dispersal of work and housing areas, utilities, and other installation support mechanisms that may require the installation to be responsible for certain areas outside of the installation perimeter.]

Appendix 1 – Jurisdictional Issues

Appendix 2 – Use of Force and/or Rules of Engagement Instructions

Appendix 3 – Pictorial Representation of Installation Jurisdiction

ANNEX I – Public Affairs (Specific PAO instructions on how to support AT operations)

Appendix 1 – Command Information Bureau Organization & Operation

Appendix 2 – Local/Regional Media Contact Information

ANNEX J – Command Relationships (Provides specific guidance on command relationships and military/civilian interoperability issues during incident command and control).

Appendix 1 – AT Organizational Charts [Crisis Management Team, AT Working Group, First Responder Elements, Incident Command Organization (include civilian and other external agencies).]

ANNEX K – Communications (Specific communications instructions on how to support AT operations. Include systems/procedures for SECURE and NON-SECURE communications means.)

Appendix 1 – Installation AT Communication Architecture

Appendix 2 – Incident Command Communication Architecture

Appendix 3 – EOC Communication Architecture

Appendix 4 – Security Force Communication Architecture

Appendix 5 – Fire Department Communication Architecture

Appendix 6 – Medical Communication Architecture

Appendix 7 – Other Agencies

ANNEX L - Health Services (Specific medical instructions on how to support AT operations)

Appendix 1 - Mass Casualty Plan

Appendix 2 - Procedures for Operating with Civilian Emergency Medical Service and Hospitals

ANNEX M – Safety (Specific safety instructions on how to support AT operations)

ANNEX N – AT Program Review, Training, & Exercises

Appendix 1 – AT Program Review
Tab A – Local Assessments
Tab B – Higher Headquarters Assessments

Appendix 2 – AT Required Training

Appendix 3 – Exercises

ANNEX O – Personnel Services. [ENTER administrative and personnel procedures required to support the plan i.e., civilian overtime, post-traumatic stress syndrome counseling.]

Appendix 1 – Operating Emergency Evacuation Shelters

ANNEX P – Reports. [ENTER all the procedures for report submissions & report format.]

Appendix 1 – Reporting Matrix

ANNEX Q – References. [ENTER all supporting reference materials, publication, regulations etc.]

ANNEX R – Distribution. [ENTER the list of agencies to receive this plan. Cover plan classification, handling and declassification procedures.]

APPENDIX 15 TO ANNEX C TO USNORTHCOM OPORD 05-01 (U)
SAMPLE RISK ASSESSMENT (U)

1. (U) The sample Risk Assessment (RA) provided describes the methodology DoD Element Commanders/Directors or designated representatives can use to assess risk. The RA combines Criticality, Threat, and VAs in order to provide a more complete picture of the risks to an asset or group of assets. In the proceeding paragraphs the RA process described does not dictate how to conduct the assessment, but rather it outlines what type of information to collect and how to organize and display the information for decision-making. A RA will assist to provide a clear picture of the current AT posture and identifies those areas that need improvement.

2. (U) The RA is a logical, step-by-step method, and shall require the participation of the entire staff. In starting the RA process, three elements should be examined:

a. (U) Threat. The threat is determined through a proper and thorough Threat Assessment (TA). The TA should identify the likelihood and severity of the terrorist to inflict injury to a person or damage to a facility or asset by considering terrorist capability, intent, and objectives. Effort should also concern specific type of weapon(s) or act(s) the terrorist will use to initiate the event (assassination, bomb, etc.).

(1) (U) The TA focuses on the full range of known or estimated terrorist capabilities in a commander's area of interest, including WMD. Commanders annually integrate threat information prepared by the intelligence and law enforcement communities, technical information from security and engineering planners, and information from other sources to prepare their TA.

b. (U) Asset Criticality. Critical assets are determined by both the term and the measure of importance to the operational mission. Areas that encompass multiple critical assets are referred to as critical areas. The criticality assessment provides information to prioritize assets and allocate resources to special protective actions.

(1) (U) The completed information may be compiled into a criticality matrix. This information is then combined with the threat and vulnerability information to assess the AT risk.

c. (U) Vulnerability. A thorough VA will highlight the susceptibility of a person, group, unit, facility, or asset to a damaging incident. VAs should also address the capabilities of response elements to plan those activities that support the ability to either deter and/or respond to terrorist threats. For example, a VA might reveal weaknesses in an organization's security system, financial management processes, computer networks, or unprotected key infrastructure such as water supplies, bridges and tunnels.

(1) (U) Local VAs should be conducted at least annually, but there should be a means to adjust the assessment as the threat changes.

3. (U) During the RA process, commanders must consider of all the aforementioned elements, to make well-informed decisions when planning FPCON measure implementation, and terrorist incident response measures.

4. (U) Assessing Risk. Assessing the risk presumes the threat, vulnerability, and asset criticality assessments have been completed.

a. (U) In addition to isolated assets, areas can be assessed in terms of the criticality of the assets located within it and its vulnerability to specific threats. The assessment team will rate each asset for every type of threat identified in the TA.

(1) (U) The process begins by creating an Asset RA Table.

(2) (U) Determine what asset to be examined.

(3) (U) Determine the attack means. Method by which the asset would be attacked. Different groups may present several different attack methods based on what weapons they possess and the methods they use.

(4) (U) Determine the vulnerability of the critical asset from the attack methods identified.

b. (U) Sample RA.

(1) (U) Installation Command Post.

(2) (U) Various groups may present several attack methods to include: small arms fire, car/truck bomb, Chemical Weapons (CW), and Biological Weapons (BW).

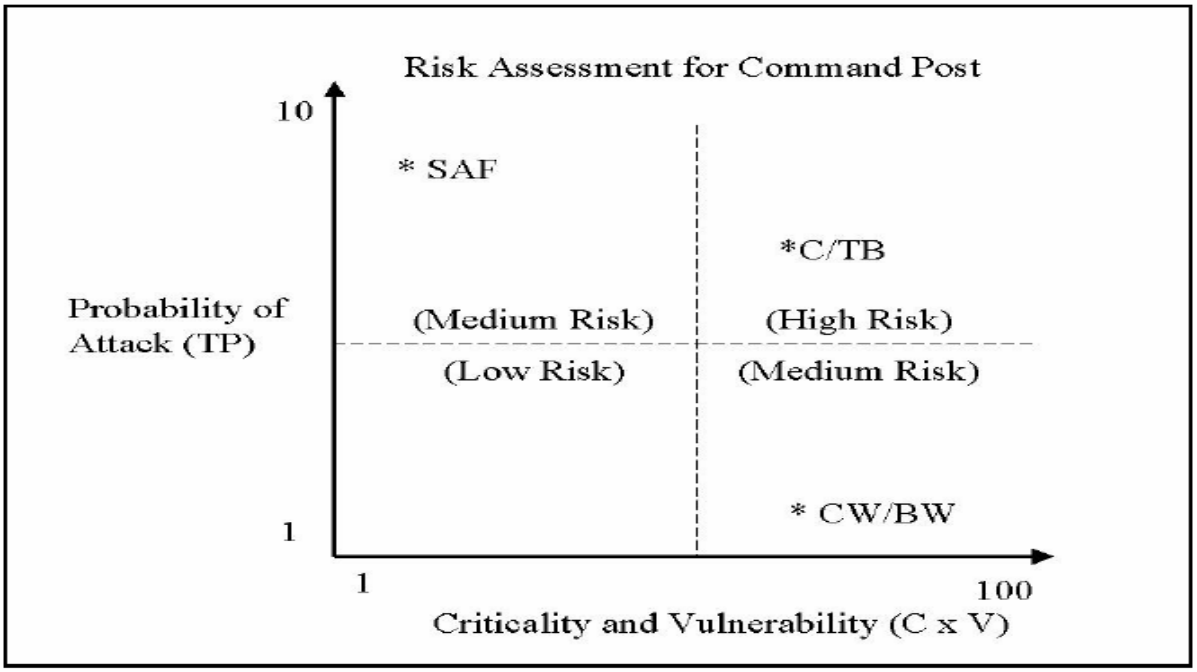
(3) (U) Vulnerabilities for the Command Post include: constructed 12” concrete walls, has no windows, and the ventilation system is not filtered. A redundant command post exists; however, several hours would be required before it could be fully operational.

(4) (U) RA Analysis. The Command Post is necessary to carry out the mission: criticality is 9 out of 10. The vulnerability is a 1 of 10 from small arms fire because small arms are unlikely to penetrate 12” of concrete and no windows exist to shoot into. The vulnerability from a car/truck bomb is higher because there is no traffic flow control around the building. The CW and BW attack means are both high vulnerabilities because the ventilation system is unfiltered (Example: Asset Risk Assessment Table below for a Command Post).

Asset: Command Post				
Attack Means	Criticality (C) (1-10)	Vulnerability (V) (1-10)	Threat Probability (TP) Y Value (1-10)	Risk Assessment (C x V x TP)
Small Arms Fire (SAF)	9	1	9	81
Car/Truck Bomb (C/TB)	9	8	6	432
CW	9	8	1	72
BW	9	8	1	72

(5) (U) It is important to note that this rating system is not meant to be a precise science. It is one method of quantifying a subjective decision, in order to generally prioritize areas in terms of risk and provide decision-makers information to determine what is an acceptable risk.

(6) (U) RA can also be presented graphically. A graph will combine the Criticality/Vulnerability/Attack Means (the x-axis) and the Threat Probability (the y-axis) to represent the risk. The representative risk is an expression of the relative impact on an asset or planning and response element, given a stated attack means. Representative risk does NOT attempt to forecast risk (e.g. assign predictability or likelihood (Example: Graphic Risk Assessment below for a Command Post).


Risk Assessment for Command Post
10
* SAF
*C/TB
Probability of
Attack (TP)
(Medium Risk)
(High Risk)
(Low Risk)
(Medium Risk)
* CW/BW
1
1
100
Criticality and Vulnerability (C x V)

For Official Use Only