

**FOR OFFICIAL USE ONLY**

**UNITED STATES EUROPEAN COMMAND**

**ANTITERRORISM – FORCE PROTECTION**

**OPERATIONS ORDER 01-01**

**30 JUNE 2001**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**FOR OFFICIAL USE ONLY**

# FOR OFFICIAL USE ONLY

HEADQUARTERS, U.S. EUROPEAN COMMAND  
APO AE 09128  
30 June 2001

## USCINCEUR AT/FP OPOD 01-01 SECURITY INSTRUCTIONS AND RECORD OF CHANGES

1. The long title of this Plan is USCINCEUR ANTITERRORISM/FORCE PROTECTION OPERATIONS ORDER 01-01. The short title is USCINCEUR AT/FP OPOD 01-01
2. This document contains sensitive information related to antiterrorism and force protection (AT/FP) of DoD elements to include personnel engaged in tactical operations in forward deployed environments. The document is marked to be handled as FOR OFFICIAL USE ONLY, and thus, all of the information contained herein must remain under the control of U.S. government. Electronic transmission of this document, to include any portion thereof, must be made over protected communications systems, e.g., the Secret Internet Protocol Router Network (SIPRNet) or higher. DoD directives strictly prohibit the transmission or revelation of information contained herein, in any manner, to an unauthorized person.
3. It is crucial that information generated and used in support of this OPOD not be over classified since it must be made readily available to all personnel and agencies responsible for AT/FP, and wide dissemination to authorized personnel serves to enhance program implementation. This is especially true in USEUCOM, where there are frequent requirements to work closely with allies and host nation authorities, as well as other non-cleared personnel, to implement appropriate measures in support of the safety and security of DoD elements and personnel. However, because of the far-reaching applicability of the requirements, care must be exercised to ensure that classified and sensitive unclassified National Defense information is not compromised. An AT/FP plan with a complete listing of site-specific AT/FP measures, linked to a Force Protection Condition, will be classified, as a minimum, CONFIDENTIAL. When separated from the AT/FP plan, specific AT/FP measures and Force Protection Conditions remain FOR OFFICIAL USE ONLY. Handling, storage and control of such information must comply with the requirements contained in DoD 5200.1-R, Information Security Program Regulation, and DoD 5400.7R, Freedom of Information Act (FOIA).
4. For additional information on classification and marking of documents generated in support of AT/FP operations, see the Security Classification Guide contained in Annex L to this OPOD. Reproduction of this document for local use, or distribution to subordinate and/or other commands is authorized.
5. This OPOD may be released to NATO member countries on a strict "need to know" basis. Further distribution outside U.S. government channels by the recipient may not be made without the express consent of the HQ USEUCOM Special Assistant for Security Matters.

**FOR OFFICIAL USE ONLY**

**6.** Based on updated threat assessments, changes in AT/FP doctrine or policies, and/or revised vulnerability assessments, the existing guidance in this OPORD may be changed by issuance of Fragmentary Orders (FRAGO), which will be posted in the Record of Changes.



# FOR OFFICIAL USE ONLY

08 March 2002

## **Fragmentary Order (FRAGO) 1 to USCINCEUR ANTITERRORISM/FORCE PROTECTION OPERATIONS ORDER 01-01, 30 Jun 2001**

Effective immediately, this FRAGO will be posted in the Record of Changes to USCINCEUR AT/FP OPOD 01-01, and the accompanying page changes will be posted within applicable areas of the OPOD.

- 1. Table of Contents.** Replace Pages v, vi and vii with the attached corresponding Pages.
- 2. Basic Order.** Replace all Pages in the Basic Order with the attached corresponding Pages.
- 3. Annex B and All Appendices thereto.** Replace all Pages in Annex B and Appendices 1 through 5 with the attached corresponding Pages.
- 4. Annex C.** Replace all Pages in Annex C with the attached corresponding Pages.
- 5. Annex C, Appendices 1 and 2.** Replace all Pages in Appendices 1 and 2 to Annex C with the attached corresponding Pages.
- 6. Annex C, Appendix 2, Tabs A and B.** Replace all Pages in Tabs A and B of Appendix 2 to Annex C with the attached corresponding Pages.
- 7. Annex C, Appendix 5.** Replace all Pages in Appendix 5 to Annex C with the attached corresponding Pages.
- 8. Annex C, Appendix 5, Tab C.** Delete Tab C in its entirety.
- 9. Annex C, Appendix 7.** Replace all Pages in Appendix 7 to Annex C with the attached corresponding Pages.
- 10. Annex C, Appendix 7, Tab A.** Delete Tab A in its entirety.
- 11. Annex D, Appendix 1.** Replace all Pages in Appendix 1 to Annex D with the attached corresponding Pages.
- 12. Annex D, Appendix 2.** Replace all Pages in Appendix 2 to Annex D with the attached corresponding Pages.
- 13. Annex D, Appendix 2, Tab A.** Replace all Pages in Tab A of Appendix 2 to Annex D with the attached corresponding Pages.

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

**08 March 2002**

**Fragmentary Order (FRAGO) 1 to USCINCEUR ANTITERRORISM/FORCE PROTECTION OPERATIONS ORDER 01-01, 30 Jun 2001**

- 14. Annex D, Appendix 2, Tab B.** Delete Tab B in its entirety.
- 15. Annex D, Appendix 3.** Replace all Pages in Appendix 3 to Annex D with the attached corresponding Pages.
- 16. Annex F.** Replace all Pages in Annex F with the attached corresponding Pages.
- 17. Annex J.** Replace all Pages in Annex J with the attached corresponding Pages.
- 18. Annex M, Appendix 2.** Replace all Pages in Appendix 2 to Annex M with the attached corresponding Pages.
- 19. Annex M, Appendix 2, Tabs A and C.** Replace all Pages in Tabs A and C of Appendix 2 to Annex M with the attached corresponding Pages.
- 20. Annex Y.** Replace all Pages in Annex Y with the attached corresponding Pages.

**OFFICIAL:**

**PETROSKY, LTG**

**CHANGE APPROVED**     **X**          **DISAPPROVED** \_\_\_\_\_

    **\\signed\\**      
**C. W. FULFORD, JR.**  
**General, USMC**  
**Deputy Commander in Chief**

# FOR OFFICIAL USE ONLY

## USCINCEUR AT/FP OPORD 01-01 ORDER SUMMARY

- 1. PURPOSE.** To establish USEUCOM policy and procedures to enhance antiterrorism/force protection (AT/FP) readiness. This OPORD fulfills the requirements contained in DoD Instruction 2000.16, DoD Antiterrorism Standards, to develop and implement a comprehensive AT/FP program. This document supersedes USCINCEUR ANTITERRORISM/FORCE PROTECTION Operations Order 99-01.
- 2. CONDITIONS FOR IMPLEMENTATION.** All DoD elements and personnel stationed or deployed in the theater who are under the force protection responsibility of USCINCEUR will implement and adhere to the policies, procedures, and standards contained herein upon the publication of this order.
- 3. OPERATIONS TO BE CONDUCTED.** All DoD elements and personnel governed by this OPORD will constantly conduct AT/FP operations to enhance the AT/FP readiness throughout the USEUCOM area of responsibility (AOR).



**FOR OFFICIAL USE ONLY****USCINCEUR AT/FP OPORD 01-01  
TABLE OF CONTENTS**

<b><u>CONTENTS</u></b>	<b><u>PAGE</u></b>
<b>SECURITY INSTRUCTIONS AND RECORD OF CHANGES</b>	i
<b>ORDER SUMMARY</b>	iv
<b>TABLE OF CONTENTS</b>	v
<b>PRESCRIPTIVE STANDARDS QUICK REFERENCE GUIDE</b>	viii
 <b>BASIC OPORD</b>	 1
 <b>ANNEX B, INTELLIGENCE</b>	 <b>B-1</b>
Appendix 1: Intelligence Support <b>Applications</b>	B-1-1
Appendix 2: Threat Analysis Methodology	B-2-1
Appendix 3: Counterintelligence	B-3-1
Appendix 4: BLUE DART Program	B-4-1
Appendix 5: Theater Threat Assessment (Classified; Published Separately)	B-5-1
 <b>ANNEX C, OPERATIONS</b>	 <b>C-1</b>
Appendix 1: Pre-deployment Requirements	C-1-1
TAB A: Training, <b>Screening</b> , and Equipment Requirements	C-1-A-1
Appendix 2: Terrorist Force Protection Conditions	C-2-1
TAB A: Force Protection Condition Measures	C-2-A-1
TAB B: Non-Controlled/Off-Installation Facility Security Strategy	C-2-B-1
TAB C: Procedures for the Use of Deadly Force	C-2-B-1-1
Appendix 3: Weapons of Mass Destruction	C-3-1
Appendix 4: United States Defense Representative (USDR) Security Responsibilities and Procedures	C-4-A-1
Appendix 5: AT/FP Forums	C-5-1
TAB A: General/Flag Officer Antiterrorism Steering Group	C-5-A-1
TAB B: USEUCOM Joint Antiterrorism Working Group	C-5-B-1
Appendix 6: Crisis Action Response	C-6-1
Appendix 7: Readiness Reporting	C-7-1
 <b>ANNEX D LOGISTICS</b>	 <b>D-1</b>
Appendix 1: AT/FP <b>Construction</b> Design Standards	D-1-1
TAB A: Sample Request for Deviation	D-1-A-1
Appendix 2: AT/FP Funding	D-2-1
TAB A: Unfinanced Requirement Request Format	D-2-A-1
Appendix 3: Combating Terrorism Readiness Initiatives Fund (CbTRIF)	D-3-1
TAB A: CbTRIF Submission Format	D-3-A-1
TAB B: Quarterly CbTRIF Report Format	D-3-B-1
TAB C: Monthly Obligations Status Report	D-3-C-1

**FOR OFFICIAL USE ONLY**

<b><u>CONTENTS</u></b>	<b><u>PAGE</u></b>
Appendix 4: Combating Terrorism Technology Requests	D-4-1
TAB A: Combating Terrorism Technology Request Format	D-4-A-1
<b>ANNEX E, SECURITY OF IN-TRANSIT FORCES</b>	<b>E-1</b>
Appendix 1: Security for In-transit Aircraft	E-1-1
TAB A: Coordinated Transient Aircraft Security Requirements	E-1-A-1
TAB B: Message Guidance for Requesting Additional Security	E-1-B-1
TAB C: Rules of Engagement/Use of Force	E-1-C-1
TAB D: Threat Working Group	E-1-D-1
TAB E: Airfield Responsibility Matrix	E-1-E-1
TAB F: Airfield Assessment Checklist	E-1-F-1
Appendix 2: Security for In-transit Ships	E-2-1
TAB A: Example of Inport Security Plan	E-2-A-1
TAB B: Example of LOGREQ Security Supplement	E-2-B-1
<b>TAB C: Example of Inport Security Plan Approval</b>	<b>E-2-C-1</b>
TAB D: Security Assessment Survey Form & Checklist Non-U.S. Ports	E-2-D-1
Appendix 3: Security for In-transit Ground Forces	E-3-1
TAB A: Assessment Checklist for In-Transit Ground Forces	E-3-A-1
<b>ANNEX F, PUBLIC AFFAIRS</b>	<b>F-1</b>
<b>ANNEX J, COMMAND RELATIONSHIPS</b>	<b>J-1</b>
<b>ANNEX K, DEFENSIVE INFORMATION OPERATIONS</b>	<b>K-1</b>
<b>ANNEX L, USEUCOM AT/FP SECURITY CLASSIFICATION GUIDE</b>	<b>L-1</b>
<b>ANNEX M, PHYSICAL SECURITY</b>	<b>M-1</b>
Appendix 1: USEUCOM AT/FP Program Standards	M-1-1
Appendix 2: Vulnerability Assessments (VA) and Program Reviews	M-2-1
TAB A: Vulnerability Assessment Management Program (VAMP)	M-2-A-1
TAB B: Component Command Assessment Checklist	M-2-B-1
TAB C: Vulnerability Assessment Checklist	M-2-C-1
TAB D: Assessment/Survey Checklists	M-2-D-1
Appendix 3: High-Risk Personnel	M-3-1
TAB A: High-Risk Personnel Transportation Support	M-3-A-1
EXHIBIT 1: Sample Request for Authority to Use Government Transportation for Unofficial Travel	M-3-A-1-1
TAB B: High-Risk Personnel (HRP) Security <b>Support</b>	M-3-B-1
TAB C: Non-Tactical Armored Vehicle Program	M-3-C-1
EXHIBIT 1: Annual Non-Tactical Armored Vehicle (NTAV) Reports	M-3-C-1-1
TAB D: Evasive Driver Training For High-Risk Personnel	M-3-D-1

**FOR OFFICIAL USE ONLY**

<b><u>CONTENTS</u></b>	<b><u>PAGE</u></b>
Appendix 4: Firearms For Personal Protection	M-4-1
TAB A: Sample Request For Authority To Bear Firearms For Personal Protection	M-4-A-1
Appendix 5: Antiterrorism/Force Protection Training	M-5-1
Appendix 6: Procedures for Screening and Handling Mail	M-6-1
<b>ANNEX Q, FORCE HEALTH PROTECTION REQUIREMENTS</b>	<b>Q-1</b>
<b>ANNEX X, DISTRIBUTION</b>	<b>X-1</b>
<b>ANNEX Y, GLOSSARY</b>	<b>Y-1</b>

## FOR OFFICIAL USE ONLY

**Table 1 USEUCOM Prescriptive AT/FP Program Standards Quick Reference Guide  
for USCINCEUR AT/FP OPORD 01-01**

(Also, each of the below listed Standards are addressed in Annex M, Appendix 1)

USEUCOM Prescriptive AT/FP Standard	LOCATION IN USCINCEUR AT/FP OPORD 01-01:
1. USCINCEUR AT/FP Policy	Basic Order
2. Development of AT/FP standards	Basic Order
3. Assignment of AT/FP Operational Responsibility	Basic Order & Annex J
4. AT/FP Coordination in Overseas Locations	Basic Order; Annex C, Appendix 1, Tab A; and Annex C, Appendix 4
5. AT/FP Program Development, Implementation and Assessment	Basic Order; Annex C
6. Assignment of AT Officers (ATO)	Annex C; Annex M & Annex M, Appendix 7
7. Application of DoD Terrorist Threat Analysis Methodology	Annex B, Appendix 2
8. Threat Information Collection and Analysis	Annex B; Annex B, Appendix 1 & 3
9. Threat Information Flow	Annex B; Annex B, Appendix 4 & Annex C
10. Potential Threat of Terrorist Use of Weapons of Mass Destruction (WMD)	Annex C, Appendix 3
11. Adjustment of Force Protection Conditions	Annex C, Appendix 2
12. Force Protection Condition Measures Implementation	Annex C, Appendix 2
13. Force Protection Condition Measures	Annex C, Appendix 2
14. Commanders shall maintain a comprehensive AT/FP Program	Basic Order; Annex M, Appendix 2
15. Terrorism Threat Assessment	Annex B, Appendix 2
16. AT/FP Risk Assessment Process and Physical Security Measures	Annex D, Appendix 1 Annex M, Appendix 1
17. Terrorism Incident Response Measures	Annex C; Annex C, Appendix 3
18. Terrorism Consequence Management Measures	Annex C, Appendix 2, Tab C & Annex C, Appendix 3
19. Training and Exercises	Annex M, Appendix 2
20. AT/FP Program Review	Annex D, Appendix 1
21. General Requirements for AT/FP Training	Annex C, Appendix 1; Annex M, Appendix 5
22. Level I AT/FP Awareness Training	Annex C, Appendix 1; Annex M, Appendix 5
23. AOR-Specific Training Requirements	Annex C, Appendix 1; Annex M, Appendix 5
24. Level II AT/FP Officer Training	Basic Order; Annex C, Appendix 1

**FOR OFFICIAL USE ONLY**

<b>USEUCOM Prescriptive AT/FP Standard</b>	<b>LOCATION IN USCINCEUR AT/FP OPORD 01-01:</b>
	& Annex M, Appendix 5
25. Training for High Risk Personnel and High Risk Billets	Annex M, Appendix 3 & 5
26. Vulnerability Assessments of Installations	Annex M, Appendix 2
27. Pre-deployment AT/FP Vulnerability Assessment	Annex M, Appendix 5
28. Construction Considerations	Annex D, Appendix 1
29. Facility and Site Evaluation and/or Selection Criteria	Annex C, Appendix 1 & Annex D, Appendix 1
30. AT/FP Guidance for Off-installation Housing	Annex D, Appendix 1 & Annex M, Appendix 1 & 2
31. Executive Protection and Protective Services	Annex M, Appendix 3

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**X**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**HEADQUARTERS, U.S. EUROPEAN COMMAND  
APO AE 09128  
30 June 2001**

**USCINCEUR ANTITERRORISM/FORCE PROTECTION (AT/FP) OPORD 01-01**

- REFERENCES:**
- a. Public Law 99-399, Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended
  - b. Public Law 100-24, Section 160, as amended
  - c. Public Law 101-246, Section 135, as amended
  - d. Section 164 and 1072(2) of Title 10, United States Code
  - e. Section 4802 and 4805(A) of Title 22, United States Code
  - f. DoD and DOS Memorandum of Understanding on Force Protection On Security of DoD Elements and Personnel In Foreign Areas, 16 Dec 97
  - g. DoD Directive 2000-12, DoD Antiterrorism/Force Protection Program, 13 Apr 99
  - h. DoD Handbook 2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence, 19 Feb 93 with Change 2
  - i. DoD Instruction 2000.14, DoD Combating Terrorism Program Procedures, Jun 94
  - j. DoD Instruction 2000.16, DoD Antiterrorism Standards, 14 Jun 01
  - k. CJCS Instruction 5261.01B, Combating Terrorism Readiness Initiatives Fund, 1 Jul 01
  - l. DoD Directive C-4500.51, DoD Non-Tactical Armored Vehicle Policy, May 87
  - m. DoD Directive 4500.54, Official Temporary Duty Travel Abroad, May 91
  - n. DoD 4500.54-G Foreign Clearance Guide, Europe
  - o. DoD 4500.54-G, V1 Foreign Clearance Guide, Africa and Southwest Asia
  - p. DoD Instruction 5105.57, Procedures for the U.S. Defense Representative (USDR) in Foreign Countries, Dec 95
  - q. DoD 5200.8-R Physical Security Program, May 91
  - r. DoD Directive 5210.84, Security of DoD Personnel at U.S. Missions Abroad, 22 Jan 92

**FOR OFFICIAL USE ONLY**

- s. DoD **Instruction** 5405.3, Development of Proposed Public Affairs Guidance (PPAG), **5 Apr 91**
- t. DoD 8910.1-M, DoD Procedures for Management of Information Requirements, 30 Jun 98
- u. CJCS Manual 3105.03, Joint Reporting Structure Event and Incident Reports, Jun 98
- v. CJCS Instruction 3213.01, Joint Operations Security,
- w. Joint Pub 1-07, Doctrine for Public Affairs in Joint Operations
- x. Joint Pub 2-01.2, Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations, Apr 94
- y. Joint Pub 3-07.2 Joint Tactics, Techniques and Procedures (JTTP) for Antiterrorism, 17 Mar 98
- z. Joint Pub 3-10, Joint Rear Area Operations, Feb 93
- aa. Joint Pub 3-10.1, Joint Tactics, Techniques, and Procedures for Base Defense, 23 Jul 96
- bb. Joint Pub 3-54, Joint Doctrine for Operations Security, 24 Jan 97
- cc. Joint Service Guide 5260, Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism, Jul 96
- dd. Air Force Instruction 31-210, The U.S. Air Force Antiterrorism Program, Jul 97
- ee. Army Regulation 525-13, The Army Terrorism Counteraction Program, Jun 92
- ff. Marine Corps Order 3302.B, The Marine Corps Antiterrorism Program, Jun 92
- gg. EUCOM Directive (ED) 55-9, Operations Security,
- hh. USCINCEUR CONPLAN 0400-96 (S)
- ii. Strategic Concept for USCINCEUR Functional Plan 4299-01, Consequence Management (S/NF)
- jj. USCINCEUR Standard Plan 4000, Mar 98
- kk. USCINCEUR Policy Letter 00-2, 2 Jan 01
- ll. USCINCEUR Policy Letter 00-3, 2 Jan 01
- mm. USCINCEUR Policy Letter 00-4, 2 Jan 01

**TIME ZONE USED THROUGHOUT THE ORDER: ZULU**



**FOR OFFICIAL USE ONLY**

**TASK ORGANIZATION:** USCINCEUR-Chief of Mission (COM) Memoranda of Agreement (MOA) that delineate AT/FP task organization are available to review on the Secret Internet Protocol Router Net (SIPRNet) via:  
<http://www2.eucom.smil.mil/hq/ecsm/MOA/moa.html>.

**1. SITUATION**

**a. General.** This order fulfills the requirement contained in DoD Standards 2, 5 and 14 of DoDI 2000.16, wherein USCINCEUR is tasked to develop, implement and maintain a comprehensive Antiterrorism/Force Protection (AT/FP) program. This order provides guidance for planning, implementation, and execution of the USEUCOM AT/FP program.

**b. Area of Concern**

**(1) Area of Responsibility (AOR).** See USEUCOM Standard Plan 4000.

**(2) Area of Interest (AOI).** Countries outside of and non-governmental actors based outside of the USEUCOM AOR that are involved in activities within and/or have influence within the AOR.

**c. Enemy Forces.** See Annex B (Intelligence), and classified Threat Assessments published under separate cover.

**d. Friendly Forces**

**(1) U.S. CINC-assigned forces**

**(2) U.S. non-CINC assigned forces**

**(3) NATO and other coalition forces**

**(4) U.S. political and diplomatic agencies and personnel**

**e. Assumptions**

**(1)** Hostile elements may target DoD personnel, supporting personnel, their families, U.S. installations, and property. Hostile elements may target DoD personnel or property for political, criminal or other intentions. These hostile elements may be indigenous to the host nation or may come from third party nations. When DoD elements and/or personnel deploy on operations or exercises, various hostile elements may look for opportunities to discredit the United States and/or the host nation, or simply seek to publicize their cause.

## FOR OFFICIAL USE ONLY

(2) DoD elements and personnel also may be at risk of harm due to collateral damage when a hostile element targets personnel or property of a host nation or other foreign nationals residing in a given host nation.

(3) DoD elements and personnel cannot rely solely on host nation support to provide necessary force protection.

(4) Terrorist attacks typically will be of brief duration. For example, terrorists will probably use hit-and-run tactics with little or no warning instead of a prolonged encounter. Also, terrorists usually will engage in extensive pre-attack surveillance of a potential target. Implementing security measures to detect this type of activity will enhance opportunities to disrupt terrorist planning and contribute to thwarting terrorist attacks.

(5) Implementation of AT/FP design standards will significantly reduce the risk of catastrophic loss of life when integrated with procedural measures into an overall installation AT/FP plan. Application of the AT/FP design 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/FP planning. The impact of incorporating AT/FP design standards into construction projects will be significantly less than the unnecessary loss of life.

(6) Individuals, groups, or countries opposed to the United States will use NIPRNet sources to obtain intelligence about the U.S. military. These actors also may attempt to infiltrate the SIPRNet and NIPRNet to disrupt or destroy information systems.

**2. MISSION.** On a continual basis, USCINCEUR executes a comprehensive AT/FP program to provide an appropriate level of safety and security for all DoD personnel, their family members, materiel, facilities, and equipment within the USEUCOM AOR, and not otherwise under the security responsibility of the Department of State, consistent with operational mission accomplishment.

### 3. EXECUTION

**Intent:** My intent is to establish a comprehensive and aggressive program to enhance the security of all DoD personnel, their families, facilities, and property against attack by terrorist/criminal groups or individuals within our AOR. We will accomplish this by implementing AT/FP measures designed to: (1) give local commanders operational control, authority, responsibility and support for force protection matters; (2) deter attack by any terrorist/criminal element through physical and operational security measures; (3) ensure intelligence provides early warning of any change in the threat; (4) ensure that procedures exist to respond to a terrorist attack should it occur; and (5) ensure all of our personnel understand the threat and their personal responsibilities in combating terrorism.

**FOR OFFICIAL USE ONLY**

**a. Force protection is one of my highest priorities.** The potential for USEUCOM forces to be exposed to terrorist activity is real. The elements are present, and given our current policy of active engagement, the question is not if we will experience an attack against our forces, but rather when. Thus, every effort must be made to deter such an attack, and force protection must become one of everyone's highest priorities.

**b.** The desired end state for our ongoing AT/FP efforts is a safer environment in which our personnel can live and conduct their operational mission(s). Our most diligent efforts may not prevent a determined terrorist attack; however, we will reduce the opportunity for such an attack and mitigate the effects of an attack should one occur.

**c. Concept of Operations.** HQ USEUCOM directs and implements AT/FP measures for CINC-assigned forces and certain designated non-CINC assigned forces. HQ USEUCOM coordinates AT/FP activities through the United States Defense Representative (USDR) with the COM, host nation police, security and military forces. AT/FP measures and activities protect DoD elements and personnel from civil disturbances, terrorist/criminal activities, and secure the facilities and equipment under our command and control. The AT/FP program consists of the following key elements:

**(1) Plans, Operations, and Exercises.** The development of comprehensive and executable AT/FP plans for installations and U.S. forces transiting the USEUCOM AOR; the review and modification of AT/FP plans as required. The incorporation of AT/FP into all operations and exercises.

**(2) Intelligence/counterintelligence.** The identification of threats; information collection; analysis of the threats, and dissemination of threat information and warnings; application of DoD Terrorist Threat Analysis methodology; and establishment of Terrorism Threat Levels.

**(3) Training and Education.** The fostering of awareness, vigilance, and caution; designation of trained Antiterrorism Officers (ATO); training on how to deal with hostage and kidnap situations; pre-deployment and AOR specific training; specialized training for personnel assigned to high-risk positions and billets.

**(4) Higher headquarters and locally conducted AT/FP program reviews and vulnerability assessments/IG inspections/Staff Assistance.** The continuing process of identifying AT/FP program shortfalls and enhancements. Inherent to this process is the establishment of mechanisms, e.g., AT/FP Working Groups, to assist in the coordinated development of AT/FP plans, prioritizing requirements, resourcing program improvements, and resolving AT/FP issues.

**(5) Physical Security.** Based on risk assessments, those measures designed to reduce vulnerabilities and provide a baseline AT/FP posture; MILCON

**FOR OFFICIAL USE ONLY**

considerations, the application of advanced technology, and implementation of sound procedures are essential elements of an effective physical security program.

**(6) Terrorist Force Protection Conditions.** (This term also is referred to as simply **Force Protection Condition (FPCON)**, and was formerly known as **Threat Conditions (THREATCON)**). Coordinated implementation of Force Protection Conditions with a mixture of protective measures, tailored to the local environment. A key feature of this system is the use of Random Antiterrorism Measures (RAM) to introduce a highly visible element of unpredictability into day-to-day operations and activities.

**(7) Operations Security (OPSEC).** Measures directed to protect security of communications systems, information activities, and personnel integrated into physical security and personal protection programs by limiting release of critical information (unclassified and classified) related to operations.

**(8) Interagency and interservice cooperation.** The sharing of information and intelligence, resources, and expertise with other U.S. government elements in the AOR.

**(9) Terrorist Incident Response Measures.** Those planned measures within each Force Protection Condition designed to respond to a broad range of terrorist threats (including WMD). The scope and extent of terrorist incident response measures will be expanded as threat levels and/or Force Protection Conditions increase. Measures will include the protection of personnel residing off of the installation or site.

**(10) Consequence Management Measures.** The wide range of emergency response and disaster preparedness actions designed to mitigate and recover from the effects of a terrorist attack. The full range of consequence management measures should include coordination with higher headquarters, other U.S. government agencies, and/or host nation authorities as appropriate.

**(11) Protection of High Risk Personnel and Protective Services.** Specialized measures designed to protect individuals and their families who may be particularly at risk.

**(12) Weapons of Mass Destruction (WMD).** Steps to identify the threat of terrorist use, vulnerability assessments, and mitigation of terrorist use of WMD options.

**d. Priority Intelligence Requirements (PIR)**

**(1)** What governments, groups, conditions, or actions pose a threat to the security and safety of U.S. forces, persons, and/or property within the AOR/AOI?

**(2)** What governments, groups, and/or individuals supporting or engaging in terrorism intend to conduct operations against our personnel or facilities? What are

**FOR OFFICIAL USE ONLY**

their motives, tactics, techniques, and procedures for supporting and/or carrying out terrorist operations? Under what conditions can/will they strike and what disincentives exist that constrain anti-U.S. terrorist groups and states from attacking? What indigenous or domestic terrorist issues pose an indiscriminate threat to our personnel?

**(3)** What countries, organizations or groups possess or are attempting to possess Weapons of Mass Destruction (WMD)? What are their objectives and targets? Which have the capability or technical expertise to produce WMD? Which have provided WMD or related equipment to others? What is the C3I profile? What situations could lead to WMD employment?

**e. Tasks and Responsibilities****(1) USCINCEUR**

**(a)** Establish command policies and an AT/FP program for the protection of all assigned and attached forces, and DoD elements and personnel for whom the CINC is assigned security responsibility by a country specific MOA pursuant to the DoD/DOS Universal MOU, reference (f). This includes family members, resources, and facilities. The AT/FP program shall include specific prescriptive standards derived from DoDI 2000.16, reference (j), that address specific terrorist threat capabilities and geographic settings.

**(b)** In accordance with the delegation of authority from SECDEF to USCINCEUR in DoDD 2000.12, reference (g), and in addition to USCINCEUR's normal exercise of COCOM and OPCON over assigned forces, USCINCEUR shall exercise TACON (for force protection) over all DoD elements and personnel (including their family members) within the AOR, except those for whom the COM retains security responsibility. The CINC's exercise of TACON (for force protection) applies to all DoD personnel in this category (and listed in Annex B of each CINC-COM MOA) assigned to, attached to, or transiting through the USEUCOM AOR. TACON (for force protection) enables the CINC to order implementation of AT/FP measures and to exercise the security responsibilities outlined in any CINC-COM MOA concluded under the terms of reference (f). TACON (for force protection) authorizes the CINC to change, modify, prescribe, and enforce AT/FP measures for all covered forces.

**(c)** Establish and maintain USCINCEUR's Operations Security (OPSEC) program to include publishing Critical Information and Essential Element of Friendly Information (EEFI) in accordance with CJCSI 3213.01, reference (v). USCINCEUR's EEFI provides overall OPSEC guidance concerning the critical classified and unclassified information that must be protected for USEUCOM to develop full spectrum AT/FP.

**(d)** Coordinate with each COM in the USEUCOM AOR to identify all non-CINC assigned forces. In coordination with the COM, review the AT/FP status of all

**FOR OFFICIAL USE ONLY**

DoD elements and personnel under the security responsibility of a COM within the USEUCOM AOR. These reviews may be conducted by the appropriate USDR with the results reported to HQ USEUCOM. In instances where AT/FP can be more effectively provided through the CINC, identify these forces as being the responsibility of the CINC in a country specific MOA, pursuant to reference (f).

**(e)** Assess and review the AT/FP programs of all DoD elements and personnel under the security responsibility of the CINC within the AOR. These assessments may be conducted by Service component commands or other subordinate commands reporting to the CINC. Relocate forces as necessary and report to SECDEF via CJCS such pertinent actions taken for force protection.

**(f)** Consistent with DoDD 5210.84, reference (r), and the Universal MOU, reference (f), serve as the DoD point of contact with host nation officials on matters involving AT/FP policies and measures.

**(g)** Provide updates to the DoDD 4500.54, references (m), (n) and (o), stating command travel requirements and theater entry requirements.

**(h)** Develop policies to fulfill AT/FP training in accordance with references (n) and (o). Develop procedures to require personnel traveling to and within the AOR comply with references (m), (n) and (o). Make unclassified security advisories in effect at time of travel available to personnel. Require that all DoD personnel and family members scheduled for permanent change of station to foreign countries receive appropriate AT/FP training prior to their departure, in accordance with DoDI 2000.16, reference (j).

**(i)** In coordination with the Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, and the Directors of the Defense Agencies, address AT/FP considerations when establishing tour lengths and determining whether restrictions should be placed on accompanying family members for personnel assigned to overseas activities. Submit recommendations to the ASD(FMP).

**(j)** Identify the requirements necessary to achieve suitable AT/FP readiness for each activity for which USCINCEUR has AT/FP responsibility. Work with other CINC, Defense Agency and Service component command executive agents as well as the USDR to satisfy these requirements in accordance with Planning, Programming, and Budgeting System (PPBS) procedures.

**(k)** Establish command relationships and policies for all DoD elements and personnel for whom the CINC has security responsibility to ensure effective mechanisms are in place to protect and defend against terrorist attack. Periodically reassess the appropriateness of command relationships of existing Joint Task Forces (JTF) and Combined Task Forces (CTF) to ensure adequate AT/FP measures are in place.

**FOR OFFICIAL USE ONLY**

**(l)** Identify and disseminate to the force providers area specific pre-deployment AT/FP training requirements that all personnel must complete before arrival in theater. Provide these training requirements to the Services and Defense Agencies for all DoD personnel and family members scheduled for permanent change of station or temporary duty to the theater. Ensure all personnel assigned or attached to HQ USEUCOM receive appropriate AT/FP training.

**(m)** Assess the terrorist threat for the theater in accordance with DoDD 2000.12, DOD 2000.12-H and DODI 2000.16, references (g), (h) and (j). Provide threat assessment and threat warning information to all DoD elements and personnel within theater as well as those scheduled to transit or deploy to the theater. On the basis of the threat assessment, identify and designate those incumbents of high-risk billets and spouses requiring AT resident training for positions not subordinate to a component commander. Notify the Service to which the incumbent is assigned of such designations, and as appropriate, code the high-risk billets to require this training prior to the incumbents arrival.

**(n)** Keep subordinate commanders and COMs informed of the nature and degree of the threat. Ensure all subordinate commanders and USDRs are prepared to respond to threat changes and rapidly transition to higher Force Protection Conditions when appropriate. Ensure the COMs are fully and currently informed of any liaison activities relating to the security of DoD elements and personnel.

**(o)** Ensure Force Protection Conditions are uniformly implemented and disseminated as specified by DoDD 2000.12, DoD 2000.12-H, and DoDI 2000.16, references (g), (h) and (j).

**(p)** Provide a representative to the DoD AT Coordinating Committee (ATCC) and its subcommittees, as required, and to the DoD Worldwide AT Conference.

**(q)** Ensure a capability exists to collect, evaluate, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack.

**(r)** For unanticipated emergency AT/FP requirements that the Services cannot fund, forward requirements to the Joint Staff in accordance with CJCSI 5261.01B, reference (k).

**(2) Service Component Commanders**

**(a)** Establish and maintain OPSEC program, to include Critical Information and EEFI in accordance with ED 55-9, reference (hh). EEFI provides commander's overall operations guidance on what critical information needs to be protected, and is critical in providing a comprehensive AT/FP program.

**FOR OFFICIAL USE ONLY**

**(b)** Designate and report to HQ USEUCOM/ECSM appropriate points of contact for planning, coordinating, and implementing all programs and initiatives related to AT/FP.

**(c)** Implement DoD, Service unique, and USEUCOM AT/FP policies and standards. Inform HQ USEUCOM/ECSM if any conflicts exist between Service unique AT/FP policies/standards and those policies/standards in this OPORD.

**(d)** Develop internal plans and policies to address AT/FP issues and requirements, as required. Service component commands may use existing plans to implement AT/FP programs. However, Service component commands must ensure that all requirements of this OPORD are incorporated.

**(e)** Require each subordinate installation or base, as well as deployed/stand alone units (e.g., battalion/squadron/ship) to assign in writing a commissioned officer, senior non-commissioned officer, or DoD civilian staff officer to be the Antiterrorism Officer (ATO). This individual will function as the commander's subject matter expert and advisor on AT/FP issues. The ATO responsibility may be a collateral or additional duty. Smaller units (e.g., company, flight, detachment) must also meet this requirement when deploying without their higher headquarters, unless deploying as a subordinate element to a unit that will have an ATO. Ensure this individual is trained to employ methods to reduce risk or mitigate the effects of a terrorist attack. The ATO is also responsible for AT/FP training and awareness within the unit. Based on the nature of the mission and the threat level, ensure units deploy the ATO early in the deployment flow of an operational mission or exercise. The ATO will conduct, supervise, assess, and report AT/FP operations as required.

**(f)** Gather, analyze, and disseminate terrorist threat information, giving particular emphasis to the rapid dissemination of terrorist threat warnings. Ensure all subordinate and/or supporting units report information on individuals, events, or situations that could pose a threat to the security of DoD personnel and resources.

**(g)** Develop and implement a process, based on terrorist threat information and/or guidance from higher headquarters, to raise or lower Force Protection Conditions. Ensure that procedures and measures for transitioning from one Force Protection Condition to another are widely disseminated and implemented. Require any changes in Force Protection Condition status to be rapidly transmitted to all DoD elements and personnel within the affected area as well as through the chain of command via OPREP reporting channels.

**(h)** Provide required resources for AT/FP requirements through Service funding channels or those of the appropriate parent command in the case of elements and personnel assigned to other CINCs or Defense Agencies.



**FOR OFFICIAL USE ONLY**

(i) Provide HQ USEUCOM/ECSM with a listing of all unfunded AT/FP requirements that meet CJCSI 5261.01B criteria, including a priority rank ordering of the items and results of the Service or parent command funding process (see Annex D, Appendix 3) **NLT 1 Feb and 1 Oct of each year**. Service component commands shall use the USEUCOM Vulnerability Assessment Management Program (VAMP) to assemble this data and prioritize their input (see Annex M, Appendix 2, Tab A).

(j) When directed, assume responsibilities as the lead Service component command for AT/FP of designated joint use facilities, exercises, and/or operations. **Further, Service component commanders shall identify AT/FP lines of responsibility for units, activities and facilities under their command to include all elements designated by CINC-COM MOA and accompanying matrix as being under the AT/FP responsibility of the Service component commander.**

(k) Conduct a comprehensive review of the command's AT/FP program and plans at least annually to facilitate enhancements and ensure compliance. For the same purpose, conduct annual AT/FP program reviews of those immediate subordinates in the chain of command. Require such reviews of their own AT/FP program and those of subordinates to be conducted by commanders at all levels at least annually. For deployed units on a less than 12-month rotational cycle, an AT/FP program review will be conducted shortly after the unit arrives in the AOR; this requirement may be satisfied by either a self-evaluation or higher headquarters program review.

(l) Ensure a higher headquarters vulnerability assessment (VA) of all subordinate commands and activities is conducted periodically with the frequency based on the current Terrorism Threat Level and/or rotation cycle, but no less than once every 3 years. Ensure this assessment meets all the requirements as stated in USEUCOM Prescriptive AT/FP Program Standard 26 (see Annex M, Appendix 1). In addition, ensure the team that conducts this assessment has the requisite expertise to evaluate all required areas (see Annex M, Appendix 2).

(m) Coordinate with HQ USEUCOM/ECSM the execution of any Service, Joint Staff Integrated Vulnerability Assessment (JSIVA), or other higher headquarters vulnerability assessment scheduled for commands and activities under the force protection responsibility of the Service component command. In addition, Service component commands **should** send a representative to accompany JSIVA or Service teams.

(n) Notify ECSM as soon as possible when scheduling and executing any off-cycle vulnerability assessments (e.g., commander-directed, installation requested). Report the results of all vulnerability assessments to ECSM using the USEUCOM VAMP on the SIPRNet. Ensure those areas that fail to meet DoD and/or USEUCOM standards for AT/FP are identified; use the reporting criteria and time lines specified in Annex M, Appendix 2.

**FOR OFFICIAL USE ONLY**

(o) Monitor the USEUCOM VAMP to ensure the accuracy of the information loaded into the system (see Annex M, Appendix 2, Tab A).

(p) Ensure the USEUCOM VAMP is updated when changes occur. Inputs to the VAMP database must include status of action, compensatory (interim) measures, and any changes to estimated completion dates. Specifically identify any recommendations regarding identified vulnerabilities the commander has elected not to implement, with rationale; otherwise provide the status of action being taken to correct the identified vulnerabilities.

(q) Based on an assessment of the threat, identify and designate those incumbents of high-risk billets and spouses requiring AT resident training. Approval authority for such designations will not be delegated below the Service component commander/deputy commander level. Notify the command providing the incumbent of such designations, and as appropriate, code such billets to require this training prior to the incumbents arrival.

(r) Prior to the deployment of any forces within the AOR or into another CINC's theater, ensure that personnel deploying conduct required pre-deployment AT/FP planning and training, and comply with all applicable instructions for AT/FP requirements.

(s) Establish a policy to govern unofficial group travel by military service members, DoD civilian employees, and family members of DoD personnel. This policy and associated program should be designed to preclude command authorized private organizations such as spouse clubs, ski clubs, or youth organizations from inadvertently planning trips to countries where the security threat poses substantial risks to American citizens. The policy should be widely disseminated and applicable to all DoD elements and personnel under the force protection responsibility of the Service component command, to include Defense Agencies and other tenant organizations. Program requirements should address as a minimum the following:

**(1) Disseminating Information.** Although the Department of State publishes travel advisories, that information may be unknown or unavailable to these groups. This information, as well as local Force Protection Conditions, should be made available for review by private organizations as a starting point for their travel planning.

**(2) Monitoring Travel.** After putting into place an effective system for disseminating information related to potential threats, procedures must be established to monitor travel of the command authorized private organizations. Constant education regarding AT/FP policies and potential threats is absolutely essential.

**(3) Prohibiting Travel and the "No Double Standard".** In cases of credible, specific and non-counterable threats, prohibiting such travel may be appropriate. Finally, adherence to the "No Double Standard" rule must be included as part of the program and clearly articulated in policy (see Annex B, Appendix 2).

**FOR OFFICIAL USE ONLY**

(t) Participate in the USEUCOM Joint Antiterrorism Working Group (JAWG) and in the General/Flag Officer Antiterrorism Steering Group (GOASG).

**(3) HQ USEUCOM Directors and Special Staff Chiefs**

(a) Participate in the GOASG.

(b) Provide membership to the Threat Working Group (TWG) with the appropriate background and expertise. Directorate (ECJ1-ECJ6) representatives must be Level II AT/FP trained, and other staff element representatives are encouraged to attend this training.

(c) Additional staff directorate responsibilities are outlined in Annex C and others as applicable.

**(4) HQ USEUCOM Special Assistant for Security Matters (ECSM).** This office is a special staff element and principal staff advisor to the CINC on AT/FP in the USEUCOM AOR and reports to USCINCEUR through the Chief of Staff and the Deputy USCINCEUR. As a special staff element, ECSM provides a direct and quick channel on all matters relating to AT/FP into the USEUCOM command group. ECSM responsibilities are enumerated in Annex C. ECSM has coordinating authority to:

(a) Ensure implementation and enforcement of DoD and USCINCEUR standards and policies for AT/FP .

(b) Assist commanders and USDRs to resolve AT/FP issues.

(c) Develop a prioritized, theater master plan for vulnerability assessments of all DoD sites and activities; provide guidance and assistance to JSIVA teams, Service component commands, and any other appropriate agencies in the execution and standardization of vulnerability assessments.

(d) Coordinate the establishment of minimum Force Protection Conditions by Service component commanders and/or USDRs, and monitor Force Protection Condition status by country, region, installation, and activity.

(e) Coordinate host nation AT/FP support at the federal/national level, through the USDR and COM, as appropriate.

(f) As proponent of this OPORD, coordinate its review with Service component commands and the USEUCOM staff on an annual basis.

(g) Through the appropriate USDR, coordinate the development of a force protection MOA with the COM of each country in the USEUCOM AOR. Conduct periodic reviews of these MOAs, to include the coordination required to update listings

**FOR OFFICIAL USE ONLY**

of DoD elements and personnel in Annexes A and B of the MOA, as required by the DoD/DOS Universal MOU, reference (f).

**(5) U.S. Defense Representatives (USDR).** Function as the single point of contact for AT/FP matters for all DoD elements and personnel under the security of the COM (see Annex C, Appendix 4).

**(6) Joint Task Force/Combined Task Force (JTF/CTF) Commanders**

**(a)** Execute AT/FP responsibilities for all forces assigned, attached, or placed under the authority of the JTF/CTF commander (TACON for force protection) by USCINCEUR. Coordinate AT/FP issues through the chain of command with ECSM, the appropriate USDR, and/or the host command/installation, as required.

**(b)** Retain OPCON for force protection of all DoD forces assigned or attached to the JTF/CTF and exercise TACON for force protection over all DoD forces deployed in support of the JTF/CTF. Execute inherent responsibilities of command for protection of forces placed under OPCON and/or TACON to the JTF (U.S. forces in the case of a CTF). USCINCEUR must approve any exceptions to retaining OPCON and/or TACON of deployed forces.

**(7) Parent Command Headquarters**

**(a)** Ensure all subordinate DoD elements and personnel who enter the USEUCOM AOR and have been placed under the OPCON or TACON of USCINCEUR comply with the AT/FP requirements of USCINCEUR and any Service component or other subordinate command exercising OPCON or TACON for force protection under the authority of USCINCEUR.

**(b)** Ensure all DoD elements and personnel deployed to the USEUCOM AOR are familiar with all requirements of this OPORD, particularly the pre-deployment AT/FP requirements listed in Annex C, Appendix 1.

**(c)** Coordinate with the USEUCOM host command to ensure AT/FP responsibilities are assigned. If deploying forces are non-CINC assigned and will be the responsibility of the COM, coordinate with the appropriate USDR to ensure that AT/FP responsibilities are assigned and clearly understood. The authority responsible for AT/FP (either the COM or USCINCEUR) must be explicitly stated in all travel orders.

**(d)** Provide funding to satisfy AT/FP requirements for units and personnel deployed to USEUCOM AOR.

**(e)** Report any forces, units, or personnel deploying to USEUCOM AOR to HQ USEUCOM/ETCC and ECSM via message.

**FOR OFFICIAL USE ONLY**

(f) Coordinate with HQ USEUCOM/ECSSM prior to conducting any Service, Defense Agency, or other AT/FP vulnerability assessment scheduled for non-CINC assigned activities/facilities. This coordination must also include the Service component command who is responsible for AT/FP at the affected activity/installation. Provide final assessment reports to HQ USEUCOM/ECSSM and the appropriate Service component command.

**(8) All supporting CINCs, Services, Defense Agencies, and the Joint Staff.** Coordinate all AT/FP initiatives and issues having an impact upon DoD elements and personnel within the USEUCOM AOR with HQ USEUCOM/ECSSM. Ensure subordinate elements rapidly report Force Protection Condition changes and terrorist threat information to HQ USEUCOM/ECSSM and all USEUCOM activities impacted by the change or information.

**(9) All Theater Clearance Authorities**

(a) Ensure AT/FP responsibility is stated in all theater clearances granted for DoD elements and personnel deploying to the USEUCOM AOR.

(b) Verify that required AT/FP training has been or will be accomplished prior to arrival in theater, and ensure that the authority responsible for AT/FP (either the COM or USCINCEUR) is explicitly stated in all travel orders. If these requirements are not satisfied, theater clearance should be denied.

**e. Coordinating Instructions**

(1) Commanders at all levels are responsible for force protection of units, activities, and facilities under their command to include those designated by CINC-COM MOA as being under the security responsibility of the commander. These responsibilities and relationships will be detailed in the CINC-COM MOA and the accompanying matrix, which shows AT/FP lines of responsibility. These documents are available on the USEUCOM Force Protection homepage and serve as the formal delegation of TACON for force protection from USCINCEUR to subordinate commanders. Further delegation to establish a clear line of responsibility through the chain of command to the installation/unit level should be accomplished by component commanders and their subordinates, as appropriate.

(2) Commanders must be proactive in the AT/FP business—commanders must study the AT/FP assessments and then visit the installations under their command. They must fix what they can and elevate items that cannot be solved at their level. Commanders must approach force protection enhancement efforts in the following manner:

**FOR OFFICIAL USE ONLY**

**(a)** Do not “sit on” issues that become bogged down due to policy or bureaucratic red tape. Local commanders need to elevate through the chain of command until resolved.

**(b)** Elevate issues that are blocked due to diplomatic impasses (host nation support) up the chain of command. If not resolved, USCINCEUR will formally notify the ambassador and SECDEF of the problem.

**(c)** When there are apparent resource limitations, first, be realistic about the nature of the problem; costs and financial requirements need to meet the common sense test. Second, elevate the total (prioritized) bill up the chain of command while working interim measures to fix the problem.

**(3)** Commanders must ensure AT/FP issues are fully integrated in determining their command’s OPSEC Critical Information and EEFI. Operations and AT/FP personnel need to cooperate fully in analyzing and evaluating operational risk.

**(4)** It is imperative that military organizations in a given country and the COM closely coordinate all AT/FP and security matters. Issues should be elevated up the chain of command to the appropriate level (normally, the Service component command headquarters or USEUCOM) specified in the terms of reference, OPORD governing the mission, or this OPORD prior to affecting direct coordination with the COM. This does not preclude direct communication when circumstances require immediate action. The USDR is the conduit to the COM for all such coordination. In conjunction with ECJ4 (only for the USDR in Turkey) and ECJ5, ECSM is the conduit between the USDR and USCINCEUR for the coordination of AT/FP issues. This does not preclude direct liaison between the USDR and other DoD agencies; however, ECSM involvement will facilitate resolution of AT/FP issues.

**(5)** DoD personnel who are under the security responsibility of the COM must meet standards developed by the DOS Overseas Security Policy Board (OSPB). When these DOS standards provide insufficient guidance for protection of DoD personnel, HQ USEUCOM ECSM and the USDR will work with the COM to augment the DOS security standards. The conflict resolution procedures in DoD Directive 5210.84, reference (r), will be applied to resolve any questions regarding the applicability of DOS and/or DoD security standards. HQ USEUCOM will use DoD/USEUCOM standards to conduct DoD required reviews of the AT/FP status of DoD activities and personnel under the security responsibility of the COM.

**(6)** To facilitate execution of this OPORD, existing MOUs/MOAs, Command Arrangements Agreements (CAAs) and other relevant agreements should be reviewed. When appropriate, such agreements will contain a reference to this OPORD. Agreements between USEUCOM subordinate commands and in-country agencies to facilitate the execution of this order are authorized.

**FOR OFFICIAL USE ONLY**

(7) Installation/activity commanders are required to take appropriate action to execute AT/FP programs for all personnel and activities under their command. In addition, local host-tenant agreements should be executed to specify both command relationships as well as AT/FP support and funding arrangements for each tenant element (whether CINC or non-CINC assigned).

(8) Service component commanders, JTF/CTF commanders, Direct Reporting Unit (DRU) commanders, and USDRs will report cases where the implementation of AT/FP guidance in this Order will adversely impact or significantly hamper accomplishment of their assigned duties. Waivers will be considered if compliance with the AT/FP standard at a particular installation, site or facility will adversely affect mission accomplishment, unacceptably affect relations with the host nation, exceed local capabilities, or require substantial expenditure of funds at a location where forces will be removed or relocated in the near future. (For additional information on processing waiver requests, see Annex D, Appendix 1.)

**4. ADMINISTRATION AND LOGISTICS**

**a. Scheme of Support.** USCINCEUR will exercise Directive Authority for Logistics (DAL) over USEUCOM assigned forces. USCINCEUR will issue directives as required to subordinate commanders to ensure effective operations execution, operational economy, and to avoid duplication. Service component commanders will provide logistics support to assigned, augmenting, and supporting units/Agencies/Services in accordance with Service directives and procedures.

**b. Logistics.** Service component commanders must be prepared to assume responsibility as lead component for logistics support at designated joint use facilities, during exercises/operations as directed. AT/FP logistics shortfalls should be reported to HQ USEUCOM ECJ4-JLOC. See Annex D.

**c. Personnel.** Personnel accountability is a major AT/FP issue. Service component commanders, JTF/CTF commanders, and Direct Reporting Unit (DRU) commanders, and USDRs must stress the importance of personnel accountability during all operational missions, exercises, TDY/TAD deployments, and day-to-day operations.

**d. Public Affairs.** See Annex F.

**e. Physical Security.** See Annex M.

**f. Medical Services.** See Annex Q.

**g. Reports.** Refer to Annex B, Appendix 3 and Annex C, Appendix 2.

**FOR OFFICIAL USE ONLY**

**h. Administration.** This OPORD supercedes USCINCEUR AT/FP OPORD 99-01. The Glossary contained in Annex Y lists definitions of terms and acronyms.

**5. COMMAND AND CONTROL**

**a.** With an AOR comprised of 91 countries, USEUCOM is unique among the Unified Commands, and management of AT/FP efforts from the headquarters in Germany presents many diverse challenges. Exacerbating the effort is the complicated command structure in the AOR, with deployed USEUCOM operational forces, security assistance activities, and numerous stovepipe organizations often functioning in the same vicinity. The SECDEF has issued guidance and direction in DoDD 2000.12, reference (g), to streamline the structure for AT/FP purposes by giving USCINCEUR TACON (for force protection) over all DoD personnel (and their dependents), except those for whom the COM retains security responsibility.

**b.** In the development of CINC-COM MOAs, there are several principles that apply in determining who should have security responsibility over DoD elements and personnel in country.

**(1)** Force protection is an inherent responsibility of command. The commander on the ground must aggressively implement all reasonable measures to ensure the force protection of the members of his/her command.

**(2)** The Chief of Mission has the ultimate responsibility for non-CINC assigned forces, and the CINC has the ultimate responsibility for CINC assigned forces. However, under the terms of the DoD/DOS Universal MOU, reference (f), the COM and CINC may agree to change operational security responsibility based on:

**(a)** Whether the COM or CINC forces are better situated to provide force protection coverage for the element or personnel in question.

**(b)** The organic force protection capabilities of the element or personnel in question.

**(c)** Given the above factors, the type of mission (does it support the COM or the CINC).

**c.** Essentially, all DoD elements and personnel in the AOR fall under one of the following categories:

**(1) CINC Assigned Forces and DRUs.** All Service component command forces fall under the command of USCINCEUR through a component commander, a JTF commander, or the senior U.S. military official within a CTF. This includes COCOM, OPCON, or supporting units specifically deployed with, or in support of operations or exercises conducted by USEUCOM through its components and/or



**FOR OFFICIAL USE ONLY**

JTF/CTF. USCINCEUR also is responsible for the force protection of DRUs, for example, Medical Flags (MEDFLAG). USCINCEUR will provide support for these forces using the best means available. Unless otherwise specified in the CINC-COM MOA, USCINCEUR retains full authority and responsibility for the protection of both CINC assigned forces and DRUs, regardless of location or mission. All theater clearances and TDY/ deployment orders must clearly indicate whether USCINCEUR or the COM is responsible for force protection, and specify local force protection contacts at the TDY site, as required by the DoD/DOS Universal MOU, reference (f).

**(2) DoD Elements and Personnel under the security responsibility of COM.**

In the absence of a CINC-COM MOA, the COM is responsible for the security of all United States Government (USG) personnel on official duty in a given country in the USEUCOM AOR, other than those DoD elements and personnel under the command of USCINCEUR, as specified in Public Law, references (a) through (e). Per the DoD/DOS Universal MOU, reference (f), DoD elements under a COM include the Defense Attaché Offices, U.S. Marine Security Guards, and Offices of Defense Cooperation (ODC). When a CINC-COM MOA is in effect, those DoD elements and personnel listed in Annex A of the MOA are under the security responsibility of the COM. The USDR is the primary military member responsible for coordination with the COM and Regional Security Officer (RSO) in each country for security issues for each of these elements and personnel. The USEUCOM AT/FP program does not usurp the COM authority and responsibility for security, but rather facilitates and assists the COM and RSO in this task.

**(3) Non-CINC Assigned Forces.** Certain non-CINC assigned forces, "stove piped" organizations representing various DoD agencies and activities, may fall under USCINCEUR for force protection. On a case-by-case basis, USCINCEUR may assume responsibility for force protection of DoD elements and personnel assigned or attached to various other operations or missions such as those under the United Nations (UN) or North Atlantic Treaty Organization (NATO). Normally, the AT/FP responsibility for these forces and individuals will be based on geographic location. The authority (either the CINC or COM) who is best situated to provide force protection support, oversight, and command & control will do so.

**(a)** In most circumstances, the Service component command (the lead component responsible for force protection) at a given location (e.g., installation, facility, or encampment) in the USEUCOM AOR will be responsible for non-CINC assigned forces deployed to or stationed at that same location.

**(b)** Under the provisions of an MOA between USCINCEUR and the COM for a given country, the appropriate USDR may be responsible for coordinating AT/FP for certain forces listed in Annex B of the MOA. The USDR will coordinate any additional support requirements necessary to accomplish this task through ECJ2, ECJ4 (only for Turkey), and ECJ5 with ECSM.

**FOR OFFICIAL USE ONLY**

(c) Situations may arise where DoD elements or personnel in a given country are not listed explicitly in a given MOA or CAA, due to exercises, TDYs, or in-transit status. Thus, all theater clearances and TDY/deployment orders must clearly indicate whether USCINCEUR or the COM is responsible for force protection.

d. SECDEF has granted USCINCEUR Tactical Control (TACON) for force protection over those Non-CINC assigned elements and personnel for whom the USCINCEUR is responsible through the execution of a CINC-COM MOA. USCINCEUR generally will delegate this authority to the appropriate subordinate commander who is best positioned to provide AT/FP support and oversight. TACON for force protection consists of the following authority:

(1) Enables USCINCEUR, or designated representative, to order implementation of force protection measures and to exercise authority over all security programs governed by the DoD/DOS Universal MOU and respective CINC-COM MOAs.

(2) Authorizes USCINCEUR, or designated representative, to change, modify, prescribe and enforce force protection measures for all DoD elements and personnel under the CINC for force protection. TACON for force protection includes the authority to inspect/assess security requirements, to direct DoD activities to identify the resources required to correct deficiencies, and to submit budget requests to parent organizations to fund identified corrections.

(3) USCINCEUR also may direct immediate force protection measures (including temporary relocation and departure) when, in his judgment, such measures must be accomplished without delay to ensure the safety of the DoD elements or personnel involved.

**e. Individuals Assigned to NATO Billets**

(1) Individuals are either on temporary duty with, or permanently assigned to, the U.S. Military Delegation to NATO. The NATO International Military Staff, SHAPE, and other such NATO billets fall under the security responsibility of the COM for the country where they are permanently assigned. The CINC and COM can agree to transfer force protection responsibility through a CINC-COM MOA.

(2) Through the execution of a CINC-COM MOA, whenever the CINC accepts responsibility over individuals assigned to NATO billets within a particular NATO element, he will delegate TACON for force protection to an appropriate local commander, normally through a Service component command.

(3) The appropriate command will coordinate AT/FP requirements with the most senior individual assigned to the NATO element in question. This senior individual will act as the representative for all other DoD personnel assigned to the NATO element in question. This representative will coordinate any AT/FP issues and requirements

**FOR OFFICIAL USE ONLY**

through his/her NATO chain of command. If issues arise where local command (a command having force protection responsibility for individuals assigned to NATO billets) AT/FP requirements come into conflict with a NATO element's requirements, every effort will be made to resolve locally any incompatibilities having an adverse impact on force protection. If unsuccessful, the representative should raise the incompatibilities through the appropriate chain of command for resolution.

**f. DoD Elements or Personnel Assigned to NATO Organizations.** U.S. forces assigned to NATO are first assigned COCOM or OPCON to USCINCEUR. These forces are then assigned NATO OPCON to NATO commanders through the transfer of authority (TOA) process. Whenever placed under the command and control of NATO, U.S. forces have two chains of authority/responsibility with respect to force protection. It is incumbent upon the U.S. commander of these forces to implement U.S. (DoD/USEUCOM) AT/FP standards.

(1) USCINCEUR has delegated OPCON of U.S. forces to component commanders, who may further delegate to subordinate commanders. Thus, the local commanders have AT/FP responsibility for those forces. U.S. commanders, under the command and control of NATO, are still required to follow all applicable U.S. rules and regulations pertaining to force protection for their personnel.

(2) As NATO commanders, the U.S. commanders have NATO OPCON (similar to U.S. TACON) of their forces, and thus, have the authority to accomplish specific tasks that are usually limited by function, time and/or location; to deploy the units concerned; and to retain or assign tactical control of those units. NATO OPCON does not include the authority to assign separate employment of components of the units, nor does it include administrative or logistic control.

(3) U.S. commanders who are dual-hatted as NATO commanders must follow USCINCEUR rules and regulations pertaining to force protection for OPCON of U.S. units. To the extent it is consistent with USCINCEUR requirements, dual-hatted commanders should provide the force protection required by NATO for NATO OPCON units. When these two sets of requirements are incompatible, dual-hatted commanders have the responsibility to implement the standards that provide the greatest security for U.S. forces consistent with mission accomplishment. In addition, every effort will be made by commands to resolve locally any incompatibilities having an adverse impact on force protection. If unsuccessful, raise the incompatibilities through the appropriate chains of command (both NATO and U.S.) for resolution.

**g. DoD Contractors.** By law and under current DoD policy, force protection 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/FP of DoD contractors or contractor employees unless specific language is included in the contract. Contractor employees, who live or work on U. S. installations, by virtue of their location, benefit from some of the same security measures provided to service

**FOR OFFICIAL USE ONLY**

members. However, contractor employees who work off base or who reside on the local economy do not receive these indirect benefits and thus must provide for their own security. In accordance with DoDD 2000.12, reference (g), and at no cost to the U.S. government, DoD contractors within the USEUCOM AOR will:

(1) Affiliate with the DOS-sponsored "Overseas Security Advisory Council" (OSAC). OSAC provides to its members threat information and training materials for use by the contractor in developing a training program for employees. The phone number for information on OSAC at DOS is 202-663-0533.

(2) Ensure that contractor employees who are U.S. nationals register with the U.S. Embassy in the country where they work. This action will place the contractor on the embassy warden system for quick receipt of threat information. Third country national employees must comply with the requirements of the embassy of their nationality.

(3) Provide AT/FP awareness information to their employees (before travel outside of the U.S.) commensurate with the information DoD provides to its military, DoD civilians and families (to the extent such information may be made available).

(4) Comply with the requirements set forth in DoD Directive 4500.54 (references (m), (n) and (o)) prior to travel outside of the U.S.

**h. Implementing Instructions.** This OPORD is effective immediately, and will be updated as required by USCINCEUR Fragmentary Orders (FRAGO). Service component commanders, CTF/JTF commanders and others reporting directly to USCINCEUR will prepare implementing instructions for this OPORD within 45 days of its published date. A copy of these implementing directives will be forwarded to HQ USEUCOM ECSM.

**ACKNOWLEDGE:**

**JOSEPH W. RALSTON**  
General, USAF

**OFFICIAL:**

**DANIEL J. PETROSKY**  
Lieutenant General, USA  
Chief of Staff

**FOR OFFICIAL USE ONLY**

**ANNEXES:**

- B. INTELLIGENCE
- C. OPERATIONS
- D. LOGISTICS
- E. SECURITY OF IN-TRANSIT FORCES
- F. PUBLIC AFFAIRS
- J. COMMAND RELATIONSHIPS
- K. DEFENSIVE INFORMATION OPERATIONS
- L. USEUCOM AT/FP SECURITY CLASSIFICATION GUIDE
- M. PHYSICAL SECURITY
- Q. FORCE HEALTH PROTECTION REQUIREMENTS
- X. DISTRIBUTION
- Y. GLOSSARY

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**ANNEX B (INTELLIGENCE) TO USCINCEUR AT/FP OPORD 01-01**

- REFERENCES:**
- a. Unified Command Plan (UCP), 29 Sep 99, [http://www1.eucom.smil.mil/ecj5/j5\\_plans/natoplans/ucp99.pdf](http://www1.eucom.smil.mil/ecj5/j5_plans/natoplans/ucp99.pdf)
  - b. Secretary of Defense Memorandum, 21 Dec 00, Subject: State-DoD Memorandum of Understanding on Security of DoD Elements and Personnel.
  - c. Executive Order 12333, 4 Dec 81, United States Intelligence Activities
  - d. Presidential Decision Directive/NSC-24, US Counterintelligence Effectiveness, 3 May 94 (S)
  - e. Memorandum of Agreement Between the Central Intelligence Agency and the Department of Defense Regarding Counterintelligence Activities Abroad, 3 Feb 95
  - f. Director of Central Intelligence Directive (DCID) 4/1, 1 Oct 86, U.S. Government Defector Program (S-NOFORN)
  - g. DCID 5/1, 19 Dec 84, Espionage and Counterintelligence Activities Abroad (S-NOFORN)
  - h. JCS Publication 2-01.2, 4 Apr 94, Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations (S-NOFORN-WNINTEL)
  - i. DoD Directive 5100.81, 5 Dec 91, Department of Defense Support Activities
  - j. DOD Directive 5105.21, 19 May 77, Defense Intelligence Agency
  - k. DoD Directive 5137.1, 12 Feb 92, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I))
  - l. DoD Directive 5148.11, 1 Jul 92, Assistant to the Secretary of Defense for Intelligence Oversight
  - m. DoD Directive 5200.27, Jan 80, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense
  - n. DoD Directive 5200.37, 18 Dec 92, Centralized Management of the Department of Defense Human Intelligence (HUMINT) Operations
  - o. DoD Directive 5210.50, 27 Feb 92, Unauthorized Disclosure of

**B-1**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

Classified Information to the Public

- p. DoD Directive 5240.6, 16 Jul 96, Counterintelligence Awareness and Briefing Program
- q. DoD 5240.1-R, Dec 82, Activities of DOD Intelligence Components that Affect United States Persons
- r. DoD Regulation 5240.1, 25 Apr 88, DoD Intelligence Activities
- s. DoD Directive 5240.2, 22 May 97, DoD Counterintelligence (CI)
- t. DoD Instruction 5240.10, 18 May 90, DoD Counterintelligence Support to the Unified and Specified Commands
- u. HQ USEUCOM Directive (ED) 40-1, 24 May 96, Intelligence - Mission and Responsibilities (S-NOFORN)
- v. HQ USEUCOM ED 40-11, 23 Aug 95, Intelligence – Counterintelligence Support (S-NOFORN-WNINTEL)
- w. USCINCEUR Standard Plan 4000, Mar 98
- x. USEUCOM Intelligence Support to Combating Terrorism (CbT) Concept of Operations (CONOPS), 20 May 98 (S)
- y. SSO EUCOM Message, DTG 200704Z OCT 00, Subject: Defense Terrorism Assessment Change Report (TACR) for the USEUCOM AOR
- z. CJCSI 8910.01, Blue Force Tracking and Dissemination Policy, 15 Dec 99
- aa. CJCSI 4110.01A, Requirements for Global Geospatial Information and Services, 15 Feb 00
- bb. CJCSI 5221.01A, Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations, 06 Apr 99
- cc. CJCSI 3141.01A, Responsibilities For The Management And Review Of Operation Plans, 15 Feb 99
- dd. CJCSI 3214.01, Military Support to Foreign Consequence Management Operations, 30 Jun 98
- ee. CJCSI 3320.01, Electromagnetic Spectrum Use in Joint Military Operations, 1 May 00
- ff. CJCSI 3610.01, Aircraft Piracy (Hijacking) and Destruction of Derelict Airborne Objects, 31 Jul 97
- gg. CJCSI 3900.01A, Position Reference Procedures, 10 Aug 98
- hh. CJCSI 6630.01A, Joint Maritime Command, Control, Communications, Computers, and Intelligence Systems

**B-2**

**FOR OFFICIAL USE ONLY**



**FOR OFFICIAL USE ONLY**

Procedures, 18 Nov 98

ii. USEUCOM Tactics, Techniques, and Procedures (ETTP) for Joint and Combined **Task Force Intelligence Operations, 31 May 2000**

**1. SITUATION**

**a. Characteristics of the Area.** The end of the Cold War opened a new set of complex regional and geo-political issues, many of which either have already required US military intervention or have the potential to do so. **Prosecution of the Global War on Terrorism (GWOT) demands increased vigilance in order to protect valuable U.S. resources and personnel.** The 11 September terrorist attacks in New York and Washington showed exceptional planning and commitment by terrorist elements whose desire is to inflict mass casualties and discredit U.S. policies. **Further complicating this situation, many countries in the USEUCOM Area of Responsibility (AOR) are in the throes of contentious and destabilizing issues such as territorial boundary disputes, ultra-nationalist and separatist movements, tribalism, political repression, religious radicalism and general political and economic turmoil.** The AOR for this plan includes all USEUCOM countries defined in reference a, and modified in references b and c to include force protection responsibility for Russia west of 100° east longitude. The wide variety of conditions throughout the AOR precludes a detailed review in this plan. Background information on specific countries/regions, including social, economic, and political factors, is contained in appropriate intelligence publications, available through INTELINK-S at <http://www.ismc.sgov.gov/> and JAC website at [http://www.jac.eucom.smil.mil/jac\\_docs/doa/t/gen-col/crisis\\_page/crisis\\_terror\\_s.html](http://www.jac.eucom.smil.mil/jac_docs/doa/t/gen-col/crisis_page/crisis_terror_s.html)

**b. Force Protection Implications.** **In addition to the force protection challenges faced in the aftermath of the tragic events of 11 Sep 01,** military contingency operations, including humanitarian assistance, non-combatant evacuation operations (NEO), peacemaking and peacekeeping deployments, numerous joint exercises, and mil-to-mil programs are major force protection challenges in the USEUCOM theater. Forward deployed U.S. military forces in the USEUCOM AOR remain vulnerable to a wide variety of threats, both to their bases in the European Central and Southern Regions and to deployment locations throughout the theater. Terrorism has been successfully employed by U.S. adversaries in the past to advance political objectives that could not be achieved through other means. That fact ensures terrorism will continue to be the "weapon of choice" of some countries, political entities, **and religious extremists** opposed to US foreign policies and military operations.

**b. Estimate of Enemy Capabilities.** Refer to Theater Terrorist Threat Assessment, Annex B, Appendix 5. Current, additional information is available through INTELINK-S up to and including **Secret** <http://www.ismc.sgov.gov/> and JAC website at [http://www.jac.eucom.smil.mil/jac\\_docs/doa/t/gen-col/crisis\\_page/crisis\\_terror\\_s.html](http://www.jac.eucom.smil.mil/jac_docs/doa/t/gen-col/crisis_page/crisis_terror_s.html). and at classification levels above Secret on JWICS INTELINK [http://www.jac.eucom.ic.gov/jac\\_docs/diss/html/crisis\\_terror.html](http://www.jac.eucom.ic.gov/jac_docs/diss/html/crisis_terror.html)

**2. MISSION.** The J2 Directorate provides USCINCEUR with timely and accurate intelligence

**B-3****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

to support his Antiterrorism/Force Protection (AT/FP) objectives as stated in this OPORD, to meet the needs of the HQ USEUCOM staff for operations, planning and threat warning, and to support the unique intelligence needs of component commands, Task Forces (TF), Joint Task Forces (JTF), Combined Task Forces (CTF), and other subordinate commands.

**3. EXECUTION****a. Scheme of support**

(1) The Director of Intelligence (ECJ2) will coordinate intelligence operations and counterintelligence activities to optimize the efforts of the component commands, collection assets and supporting agencies to satisfy Priority Intelligence Requirements (PIR) contained in paragraph 3(d) of the Basic Order.

(2) USEUCOM intelligence organizations collect, process, analyze, produce, and disseminate intelligence pertaining to terrorism in the AOR/AOI in order to present clear, tailored, accurate, and timely analysis of the situation to the supported task force commander/components, regardless of structure, size, or scope of operations. Intelligence is provided through a theater-wide network of joint, component, and combined intelligence centers and liaison elements. USEUCOM also depends on national-level resources for intelligence which is either beyond the capability of assigned intelligence resources to collect or produce, or which is a delegated responsibility of other national intelligence community producers. Intelligence support activities are described in references (c) and (d).

(3) **Allied/Coalition Operations.** When U.S. forces are under the Operational Control of NATO or coalition command, HQ USEUCOM will continue to ensure U.S. national intelligence support is provided in concert with the intelligence resources of allied nations. All possible efforts should be made to integrate the resources of allied/coalition partners.

(4) **Planning and Direction.** Theater intelligence analysis and production activities have been consolidated at the Joint Analysis Center (JAC). **Standard** request for information (RFI) that cannot be handled at or below the task force level is forwarded to the JAC via COLISEUM where it is acted upon or forwarded to the Defense Intelligence Agency (DIA) for centralized, national-level assistance or collection. The goal at all levels is to tailor the response to meet the operator's needs.

(5) **Theater Terrorist Threat Assessments.** The Joint Analysis Center's **Counter Terrorism/Counter Intelligence (CT/CI) Division (JAC/DOX)** produces terrorist threat assessments. Assessments are generally classified and can be found on the USEUCOM Joint Analysis Center (JAC) homepage on the SIPRNET INTELINK-S at <http://www.jac.eucom.smil.mil/> with additional information derived from more sensitive intelligence sources and methods available on the JAC homepage on Joint Worldwide Intelligence Communications System (JWICS) INTELINK at <http://www.jac.eucom.ic.gov/>. To request tailored threat assessments, submit a Request for Information (RFI) as outlined in paragraph 3a(8)(b), below.

**FOR OFFICIAL USE ONLY**

**(6) Terrorism Threat Levels and Warning Reports.** Defense Intelligence Agency (DIA) establishes a DoD Terrorism Threat Level to identify the potential risk to DoD personnel in a particular country. DIA and/or the Joint Analysis Center will issue Defense Terrorism Warning Reports to indicate terrorist groups are operationally active and specifically targeting U.S. interests. ECJ2 (JAC) will prepare Terrorist Threat Assessments to provide a more granular assessment of the terrorist threat to particular installations and personnel within the USEUCOM AOR. These assessments will be made available on the JAC homepage at the addresses above.

**(7) Medical Threat Assessments.** Medical intelligence personnel or Service equivalent provide medical input for threat assessments. One source of medical threat advisories is available through the **Defense Intelligence Agency's Armed Forces Medical Intelligence Center (AFMIC)**, available on SIPRNET at <http://www.dia.smil.mil/intel/afmic/afmic.html>. Requests for Information (RFI) should be submitted as outlined in paragraph 3a(8)(b), below.

**(8) Requirements.** During all phases of any operation, new intelligence requirements should be generated as the political, military, and operational situation changes in and around the USEUCOM AOR/AOI.

**(a) Essential Elements of Information (EEI).** See Appendix 1 of EUCOM Standard Plan 4000 for general guidelines. See other plans, as applicable, for specific EEI pertaining to particular military operations.

**(b) Requests for Information (RFI)** will be submitted through the Community On Line Intelligence System for End-Users and Managers (COLISEUM). By using COLISEUM, requests are forwarded to the organization best able to assess the threat **and also allows other customers to have access to the information provided.** If your organization does not have access to COLISEUM, forward RFI through your next echelon intelligence office to the USEUCOM Joint Analysis Center (JAC), RAF Molesworth.

**(1)** Submit RFIs through the supporting service component intelligence office.

**(a)** Army Elements: US Army, Europe (USAREUR/DCSINT)

**(b)** Navy Elements: US Naval Forces Europe (NAVEUR/N2)

**(c)** Air Force Elements: US Air Forces Europe (32 AIS)

**(d)** Marine Corps Elements: US Marine Corps Forces, Europe

(MARFOREUR/G2)

**(e)** Joint Organizations: HQ USEUCOM/J2

**(f)** Joint Task Force (JTF): JTF J2

**(g)** Combined Task Force (CTF): CTF C2

**(2)** Submit RFI for tailored threat assessment at least ten (10) working days prior to routine deployment.

**(3)** Provision of telephonic or email advance notice to ECJ2 and the JAC is encouraged, but not in substitution of COLISEUM procedures.

**(4)** Crisis action RFIs should be made telephonically to JAC at STU III DSN 268-

**B-5**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

2237 or during non-duty hours at 268-2235. Telephonic RFIs should be followed up with a COLISEUM entry as soon as possible.

**(9) Intelligence Surveillance & Reconnaissance (ISR) Management: Theater Roles and Responsibilities.** With the exception of assets delegated to components or JTFs, HQ USEUCOM retains tasking authority for all sensor platforms when deployed in theater. When tasking authority is delegated downward, HQ USEUCOM retains the ability to request subordinate units assistance with target satisfaction. Component commands and JTFs are required to provide target decks for their platforms to the European Collection Management Office-Airborne (ECMO-A) at least 24 hours prior to mission execution enabling theater planners to deconflict targets and airspace.

**(a) ECJ2:** On behalf of USCINCEUR, ECJ2 exercises theater airborne collection management (CM) through the ECMO-A at JAC Molesworth; provides CM policy to theater components, JTFs and supporting units/agencies; establishes command and control relationships for CM organizations; oversees theater CM planning in support of joint/combined operations; and, ensures appropriate ECMO-A manning.

**(b) HQ USEUCOM ECJ23-ISR:** Serves as the staff proponent for airborne ISR management and policy in theater; interacts regularly with the USEUCOM JRC, ECMO-A, theater components, JTFs and supporting units/agencies on plans and policy for airborne ISR missions and tasking; and, advises the ECJ2 on significant issues involving the use of airborne ISR assets, requirements and shortfalls in theater.

**(c) HQUSEUCOM J33 JRC:** Operates as the functional director, scheduler and controller is ISR platforms IAW overall USCINCEUR priorities.

**(d) JAC:** Provides Collection Management and collection oversight through the ECMO-A; focal point for dissemination and storage of secondary imagery products; theater Request for Information (RFI) manager; and, provides imagery exploitation support as needed.

**(e) ECMO-A:** Provides timely and efficient nomination, validation, prioritization, tasking, resource management, and exploitation tasking of intelligence from airborne ISR platforms assigned to or operationally controlled by USEUCOM; coordinates with USEUCOM J23-ISR, J33-JRC, theater components, JTFs and supporting units/agencies on airborne ISR missions and tasking.

For more specific direction on intelligence collection, see Appendices 1, 2, 3, 5, 7 and 8 to Annex B of USEUCOM Standard Plan 4000, reference (w).

**(10) Processing and Evaluation.** The JAC and component intelligence centers support intelligence processing within the European theater. See USEUCOM Standard Plan 4000 for information regarding processing of information from a particular intelligence discipline.

**FOR OFFICIAL USE ONLY**

**(11) Production.** The JAC Analysis Division (JAC/DOA) is the theater focal point for all-source intelligence analysis and reporting. Analytical assessments include Military Capabilities Studies, Political/Military Assessments, Forecasts and Estimates, Economic/Social/Cultural Issues, Biographies, support to I & W, current intelligence products and Special Assessments. Reporting is made available to operational users at various classification levels via INTELINK (SCI), INTELINK-S (Secret/Collateral-level and below), GENSER (Secret/Collateral-level and below) and DSCS (SCI) message traffic, and the Linked Operational-Intelligence Centers Europe (LOCE) system for NATO-releasable, collateral information.

**(12) Dissemination**

**(a)** Service component commands are responsible for forwarding threat warning to service members deployed in the USEUCOM AOR.

**(b)** DoD elements and personnel deploying to the USEUCOM theater must coordinate with the corresponding Service component command in order to establish procedures to receive immediate threat warnings. Component commands are responsible for providing required 24 hour contact information for the transmission of imminent terrorist threat information to the JAC DOX Counterterrorism Watch prior to deployment. The CTW JWICS email is [CTW@jac.eucom.ic.gov](mailto:CTW@jac.eucom.ic.gov) and on SIPRNET at [ctw@jac.eucom.smil.mil](mailto:ctw@jac.eucom.smil.mil). The CTW Watch Officer phone number is DSN 268-2487, Commercial 44-1480-2487.

**(c)** The USEUCOM Joint Analysis Center and HQ USEUCOM have twenty-four hour Intelligence Centers to provide immediate threat warning, based on intelligence reporting. The JAC issues terrorist threat warnings via record message traffic spot reports or via phone, email or radio contact as appropriate. The JAC is the Theater Indications and Warning point of contact. The Intelligence Operations Center (IOC) serves as the 24/7 coordination center of intelligence operations for the USEUCOM Director of Intelligence, orchestrating intelligence support to ongoing operations and deployed elements. The IOC acts on behalf of the USEUCOM J2 in order to initiate and task immediate intelligence requirements in support of current operations. Contact information is as follows:

**(1)** JAC JOC Watch contact information: JWICS email address is [jacjwc@jac.eucom.ic.gov](mailto:jacjwc@jac.eucom.ic.gov). Siplrnet email address is [jocwatch@jac.eucom.smil.mil](mailto:jocwatch@jac.eucom.smil.mil). The JAC I&W Watch Chief's phone number is dsn 268-2069. Red switch is 268-2235. Commercial is 44-1480-842-235.

**(2)** IOC contact information: the USEUCOM IOC is now using [USEUCOM IOC@hq.eucom.ic.gov](mailto:USEUCOMIOC@hq.eucom.ic.gov) as its JWICS email address. Effective 1 Mar 2002, the IOC will transition from using its current Siplrnet email address ([j2watch@eucom.smil.mil](mailto:j2watch@eucom.smil.mil)) to [USEUCOM IOC@eucom.smil.mil](mailto:USEUCOMIOC@eucom.smil.mil). The USEUCOM Senior Intelligence Director's phone number is dsn 430-8135. Red switch is 432-2235. Commercial is 49-711-680-8135.

**(d)** The JAC Counterterrorism Watch (JAC/CTW) will conduct monthly terrorist threat warning exercises to validate the theater warning infrastructure. Threat warnings are also forwarded via bulletins on SIPRNET or JWICS e-mail to pre-formatted threat warning

**FOR OFFICIAL USE ONLY**

address lists. Contact USEUCOM ECJ23 Intelligence Operations Center (DSN 430-5689) or SIPRNET to be added to these e-mail lists. In the event of a loss of communications with JAC/CTW, USEUCOM ECJ23-IOC will assume responsibility for threat warning.

(e) Primary intelligence dissemination will be through the interconnected theater and component intelligence facilities. The JAC will be the primary theater source of U. S. intelligence support to USCINCEUR and to NATO SACEUR via the SHAPE Survey Section and the two Joint Operational Intelligence Centers (Deployed intelligence teams). Component commands will provide tailored air, ground, and maritime/ amphibious intelligence to their supported commanders and to the JAC. The JAC, in turn, will provide fused, all-source analyses and assessments to the components for use in their service-unique tactical applications.

(f) Intelligence reports required from units. Refer to USEUCOM Standard Plan 4000.

(g) Formats for intelligence reports. Refer to EUCOM Standard Plan 4000. Also refer to Appendix 4 (BLUE DART Program) of this Annex.

(h) Requirements for releasability to allied nations. To assist host nation security forces and accommodate the flow of intelligence to allies, the dissemination function must include sanitation, decompartmentation, and releasability mechanisms. USEUCOM Foreign Disclosure Office (FDO) provides overall disclosure policy guidance. JAC and component FDOs implement and are responsible for the sanitization and disclosure of their organization's products. Additional information is available through the Foreign Disclosure Home Page at: [http://www.jac.eucom.smil.mil/jac\\_docs/dsp/fdo/FDO\\_home.html/](http://www.jac.eucom.smil.mil/jac_docs/dsp/fdo/FDO_home.html/)

(h) Requirements for secondary imagery dissemination. Refer to Appendix 7 of EUCOM Standard Plan 4000.

**b. Tasks to subordinate units****(1) HQ USEUCOM ECJ2**

(a) Provide current terrorism intelligence support to the HQ USEUCOM Battle Staff.

(b) Provide current terrorism intelligence support to Components, Sub-Unified Commands and military elements operating within or transiting through the USEUCOM AOR.

(c) Manage and provide continuity for U.S. national intelligence support for USEUCOM.

(d) Direct, coordinate and deconflict the theater multidisciplinary intelligence collection effort.



**FOR OFFICIAL USE ONLY**

(e) Validate and forward theater requirements for U.S. national systems.

(f) Manage theater target development, target databases, target materials, weapons systems effects, and computational systems support programs.

(g) Manage theater GIS support programs and validate requirements submitted by component commands.

(h) Provide intelligence staff personnel to Force/JTF Commander as directed.

(i) Provide Indications and Warning support to HQ USEUCOM, with analytical input from the JAC.

**(2) USEUCOM Joint Analysis Center (JAC)**

(a) Provide Theater Antiterrorism/Force Protection (AT/FP) over watch and immediate threat warning to HQ USEUCOM, component and sub-unified command headquarters, and attached elements 24 hours per day, 7 days per week (24/7).

(b) Provide tailored all source AT/FP intelligence to Task Force commanders and assigned forces.

(c) Direct, coordinate and de-conflict JAC and Task Force all-source intelligence collection efforts and focus requirements for theater/national systems tasking.

(d) Provide timely terrorist threat assessments, including military intent, capability, and political sensitivity to HQ USEUCOM, Task Force commanders and assigned forces.

(e) Manage and respond to Requests for Information (RFIs).

(f) Provide tailored terrorist threat assessments in support of U.S. and Allied force deployments and forces in transit.

(g) Provide AT/FP intelligence in a form releasable to host nation security elements.

(h) Provide manning augmentation to U.S. National Intelligence Cells (USNIC) and Task Force headquarters, as directed.

(i) Forward terrorist threat intelligence collected by subordinate elements to HQ USEUCOM ECJ2.

**(3) Service Component Commanders**

**FOR OFFICIAL USE ONLY**

(a) Collect, analyze, produce and disseminate theater wide multi-disciplined intelligence on terrorist threats to their installations/facilities/sites, deploying forces, and all other DoD elements and personnel transiting to, from or through the USEUCOM AOR in accordance with Component Priority Intelligence Requirements (PIR), established force protection mission requirements and USCINCEUR priorities. Dissemination will be tailored to the requirements of the receiving U.S. command. The component commands should maintain the multi-disciplined intelligence they collect in tactical databases, overlaying their data on the JAC-provided theater wide baseline.

(b) Provide intelligence support (analytical, systems, manning) to USCINCEUR and U.S. Deployed intelligence teams as directed.

(c) Establish and sustain capability to forward Immediate Threat Warning (ITW) to subordinate or attached elements 24 hours per day, 7 days per week (24/7).

(d) Forward terrorist threat intelligence collected by subordinate elements to HQ USEUCOM J2 and Joint Analysis Center.

(e) Inform JAC CTW, DSN 268-2487, of planned service deployments or forces in transit at earliest opportunity in accordance with Annex E of this OPOD.

(f) Coordinate support to USCINCEUR from service intelligence and counterintelligence organizations as shown below:

(1) For USAREUR, US Army Intelligence and Security Command (INSCOM).

(2) For USNAVEUR, Office of Naval Intelligence (ONI); Naval Security Group (NSG); and Naval Criminal Investigative Service (NCIS).

(3) For USAFE, Air Intelligence Agency (AIA) and Air Force Office of Special Investigations (AFOSI).

(4) For MARFOREUR, Headquarters U.S. Marine Corps, Intelligence Department.

(5) For SOCEUR, U.S. Special Operations Command (USSOCOM).

(4) **CINCUSNAVEUR.** Coordinate with USCINCLANT and USCINCPAC for intelligence support to Navy and Marine Corps forces operating in the Atlantic and Indian Oceans in support of USEUCOM.

(5) **COMMARFOREUR.** Provide support to USNAVEUR on intelligence planning considerations and capabilities as they relate to U.S. Marine Forces OPCON to USNAVEUR.

### c. Coordinating Instructions

(1) Intelligence capabilities available to support USCINCEUR AT/FP program objectives include national assets as well as those of the Services, other CINCs and allied commands. The following provides an overview of these capabilities and the various roles of other supporting organizations:



**FOR OFFICIAL USE ONLY**

**(a)** National level intelligence organizations, including Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Security Agency (NSA) and National Imagery and Mapping Agency (NIMA), may provide the following:

- (1)** Intelligence on terrorist groups operating within the USEUCOM AOR.
- (2)** Intelligence on transnational terrorist groups who transit through or conduct operations that impact the USEUCOM AOR.
- (3)** Intelligence on terrorist activities that could impact assets or facilities of nations within the USEUCOM AOR.
- (4)** Where compartmented programs or sensitivity limits the distribution of intelligence products, compartmented access may be given to Joint Analysis Center terrorism analysts (JAC/DOX) to assist in shaping analysis.
- (5)** Notification to the USEUCOM JAC Counterterrorism Watch, DSN 268-1410, of deployments to or transit through the USEUCOM AOR.

**(b)** Federal Bureau of Investigation (FBI). Through appropriate liaison activities, the FBI may provide terrorism related information for countries within the USEUCOM AOR, or information on transnational terrorism that could affect the USEUCOM AOR.

**(c)** Other CINCs and Services play a key role in supporting the USEUCOM intelligence effort by providing the following:

- (1)** Coordination with USEUCOM JAC Force Protection Watch to provide intelligence to assigned forces in transit prior to CHOP to or from, or transit through the USEUCOM AOR.
- (2)** Intelligence on transnational terrorist groups within USCENTCOM AOR that transit through, or conduct operations that impact the USEUCOM AOR.
- (3)** Intelligence on terrorist activities that could impact assets or facilities of nations within the USEUCOM AOR.
- (4)** Where compartmented programs or sensitivity limits the distribution of intelligence products, every attempt will be made to grant access to Joint Analysis Center terrorism analysts (JAC/DOX) to assist in shaping analysis.

**(d)** USJFCOM. Provides capability for intelligence support to USCINCEUR assigned naval forces operating in the Atlantic Ocean.

**(e)** USCINCPAC. Provides capability for intelligence support to USCINCEUR assigned naval forces operating in the Indian Ocean.

**(f)** U.S. Regional Joint Operational Intelligence Cells are a key link during NATO related operations and may provide the following:

- (1)** NATO-releasable intelligence to supported NATO major subordinate commands – AFSOUTH and AFNORTH. Support will be specifically tailored to the supported commands operational intelligence requirements. The component commands should maintain the multi-disciplined intelligence they collect in tactical databases, overlaying their data on the JAC-provided theater wide baseline.

**FOR OFFICIAL USE ONLY**

(2) All source intelligence collection and analysis on enemy ground, maritime and air operations to Force/JTF Commander in accordance with USCINCEUR priorities. Support will be specifically tailored to the supported commander's operational intelligence requirements.

(3) Feedback on operational commanders' mission planning objectives to other U.S. intelligence production elements to facilitate better focus for reporting.

(g) Allied and Coalition Forces. See specific Operations Plan for the given coalition operation.

**(2) Consolidated Listing and Impact Assessment of Shortfalls and Limiting Factors.** Shortfalls and factors which limit intelligence support during crisis situations degrade the ability to collect, process, analyze, produce, and/or disseminate complete, accurate, and timely intelligence to theater commanders and deployed U.S. and allied/coalition forces. Shortfalls and limiting factors may involve the following:

(a) Lack of collection placement and access against the terrorist target set. Terrorist operations tend to be highly compartmented, based on person-to-person communications and exercise effective operations security.

(b) High-level classification and compartmentation of intelligence and operational information on terrorism at the national level limits information available to the Theater.

(c) Limitations on communications support, such as capacity, vulnerability to disruption or destruction, quality (such as lack of suitable, indigenous landlines to support secure telephones,) interoperability with allied or coalition systems, and availability of spare parts and qualified maintenance personnel.

(d) Readiness issues such as a widespread training deficit for a new system or lack of essential equipment or supplies for deployment (such as maps and charts).

(e) Organizational problems such as duplication of responsibilities, cumbersome coordination procedures, or disagreement among coalition members concerning required intelligence support.

(f) Adverse field conditions, such as vulnerability of intelligence personnel and equipment to sniper fire or other attack, or lack of coalition support (either in terms of cooperative intelligence exchange or life support issues).

(g) Manning shortfalls, either in terms of sustaining a prolonged deployment, a shortage of specialized skills (such as linguists with a particular language capability), or lack of experience level (such as preponderance of recent cross-trainees).

(h) Limitations on available intelligence support systems, such as reliability, capacity, number of units supporting the scope of deployment, degree of integration with other systems, ease of operation, degree of mobility, interoperability with allied systems, and

**FOR OFFICIAL USE ONLY**

availability of spare parts and qualified maintenance personnel.

(i) Diversion of effort. Because intelligence forces possess unique capabilities (linguistic, communications, graphic presentation, situational awareness, etc), intelligence forces are sometimes diverted away from predicting activities of enemy forces toward other military activities.

**(3) Resolution of listings of Shortfalls and Limitations**

(a) Supporting organizations assessments of shortfalls or limiting factors should include both the probable, negative impact on intelligence support to deployed forces and the possible degradation of theater intelligence capabilities. Additionally, state the specific overall impact resulting from a combination of factors (e.g., lack of knowledgeable sources with access to terrorist information or inability to gain RELEASABLE intelligence for Host Nation Forces).

(b) These assessments should be sent to appropriate senior command elements for submission to J-2 for evaluation and dissemination to the appropriate agency to address and resolve.

(4) Specific details concerning a unit's shortfalls and limiting factors generally are classified at least CONFIDENTIAL. Consult appropriate security directives and source documents for guidance concerning specific issues.

(5) See Annex B to specific USCINCEUR plans for shortfalls and limiting factors affecting particular military operations.

(6) See Annex B of EUCOM Standard Plan 4000 for information regarding the following intelligence programs: Essential Elements of Information (Appendix 1); Signals Intelligence (SIGINT) (Appendix 2); Targeting (Appendix 4); Human Resources Intelligence (HUMINT) (Appendix 5); Intelligence Support to Information Operations (Appendix 6); Imagery Intelligence (IMINT) (Appendix 7); Measurement and Signatures Intelligence (MASINT) (Appendix 8); Captured Enemy Equipment (Appendix 9); and Intelligence Augmentation Teams (Appendix 10).

**FOR OFFICIAL USE ONLY**

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
**General, USAF**

**APPENDICES:**

1. Intelligence Support Applications
2. Terrorist Threat Analysis Methodology
3. Counterintelligence (CI)
4. BLUE DART Program
5. Theater Terrorist Threat Assessment

**FOR OFFICIAL USE ONLY****APPENDIX 1 (INTELLIGENCE SUPPORT APPLICATIONS) TO ANNEX B (INTELLIGENCE) TO USCINCEUR AT/FP OPOD 01-01**

**1. PURPOSE.** To provide information on what Intelligence Support Applications can be used in support of Antiterrorism/Force Protection (AT/FP). Because NATO allies often will have other insights into Force Protection issues, analysts should not ignore NATO classified systems, like LOCE, for the opportunity to gain additional perspectives.

**2. APPLICATIONS.** The next paragraphs discuss five noteworthy applications on classified systems that directly support AT/FP operations. An analyst should also use Intelink, AMHS, and unit homepages for additional information on JDISS, SIPRNet, and LOCE. Along these lines, the very first place to look would be the JAC homepage, where the JAC Terrorism/Counterintelligence Division (DOX) maintains an actively updated web page at: JDISS: <http://www.jac.eucom.ic.gov/jac-docs/doa/t/doctypeindex.html> and at SIPRNET: <http://www.jac.eucom.smil.mil/jac-docs/doa/t/genscol/doctypeindex.html>. The JAC EUCOM Force Protection Summary (JEFPROS) is also available from the JAC web page at [http://www.jac.eucom.smil.mil/jac\\_docs/doa/t/gen-scol/doctypeindex.html](http://www.jac.eucom.smil.mil/jac_docs/doa/t/gen-scol/doctypeindex.html).

**a. Community On-Line Intelligence System for End Users and Managers (COLISEUM).** COLISEUM supports the DoD Intelligence Production Program (DoDIPP) mission to "consolidate and gain synergism of DoD intelligence production resources" by automating its key operational concepts. It automates assignment of production requirements, and assigns production requirements based on area of responsibility. It also assigns a single primary producer, although multiple collaborative producers may be used. All Requests For Information (RFI) must be submitted via this system.

(1) JDISS European login page: <http://colhgaeucom.ic.gov/>

(2) JDISS DC login page: <http://www.coliseum.ic.gov/coliseum/app>

(3) SIPRNET: <http://coliseum-s.dia.smil.mil/>

(4) LOCE: planned for FY02

**b. InfoWork Space (IWS).** This is a free software package engineered for both corporate and military environments. It is intended to revolutionize the way groups and individuals collaborate in day-to-day mission operations. This software allows an organization to reconstruct their environment into a virtual model and then operate within that model just as in actual life. IWS allows users to collaborate in virtual on-line meeting rooms using voice or text chat. Users can share data (Documents, Whiteboard). Other uses include communications such as desktop conferencing (asynchronous and real-time), distance learning, mass briefing, and knowledge management. IWS is intended for users who require secure on-line communications

**FOR OFFICIAL USE ONLY**

and data sharing tools. POC is USEUCOM ECJ25-S at DSN 430-5641. IWS accounts can be requested at:

(1) **JDISS:** <http://hqiws.hq.eucom.ic.gov> (Open only from JDISS)

(2) **SIPRNET:** <http://hqiws.eucom.smil.mil>

(3) **LOCE:** <http://iws1.loce.eucom.smil.mil>

**c. The USAFE Risk Assessment Management Program (RAMP)** is a program identifying possible threats on all approved airfields in the USEUCOM AOR. **RAMP** describes the terrorist, criminal, and foreign intelligence threats for the airfield and local area. The RAMP format is being adopted by USEUCOM as the J-RAMP in the near future. The intent is for the J-RAMP to serve as the primary intelligence tool for forces transiting through the USEUCOM AOR. USAFE RAMP can be found on SIPRNET at <http://coldfusion.ramstein.af.smil.mil/RAMP/index.cfm> or at DSN 480-7113/6871. After duty hours, call the USAFE Intelligence Operations Center, DSN 480-6871.

**d. The Joint Threat Reporting and Analysis Capability - Europe (JTRACE)** is a government developed software tool and database which allows SIPRNET and JDISS users in theater to report possible threat incidents and events via a web portal. The tool is also available to NATO allies via LOCE and in the future Commonwealth members via the Stone Ghost system. The tool allows users to input, review, update, retrieve, and analyze reporting in a collaborative environment. The tool supports ongoing force protection and counterterrorism operations. It is maintained by the Joint Analysis Center for the component services and is planned to replace service specific reporting databases such as USAREUR's Central Region Threat Database.

(1) **JDISS:** <http://epoint.jac.eucom.ic.gov/JTRACE/> (Open only from JDISS)

(2) **SIPRNET:** <http://epoint.jac.eucom.smil.mil/JTRACE/>

**e. Analyst's Notebook and iBase** are commercial software applications developed to assist investigative analysis. Analyst's Notebook assists analysts uncover, interpret, and display complex information in a graphical form. It provides multiple views into the data, assisting identification of connections between related sets of information and revealing patterns in the data. These views are displayed as charts, including link analysis and timeline or sequence of events. Charted items link directly to the data records contained in iBase, the accompanying database. iBase is a database system fully integrated with the Analyst's Notebook application and is designed to rationalize and collate data from a diverse range of sources into a single coherent structure organized to meet specific requirements established by JAC Counterterrorism and Counterintelligence analysts. The Joint Analysis Center is working with US Army, Europe on creating a single iBase database environment for common use within theater. The analysis and database software must be installed on individual analysts' workstations, is license based, and is not freely accessible. However, the link charts

**FOR OFFICIAL USE ONLY**

resulting from analysis can be viewed by any customer using the freeware Link Chart Reader installed as part of the USEUCOM NT software baseline.

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
General, USAF

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)



**FOR OFFICIAL USE ONLY****APPENDIX 2 (THREAT ANALYSIS METHODOLOGY) TO ANNEX B  
(INTELLIGENCE) TO USCINCEUR AT/FP OPOD 01-01****1. DoD TERRORIST THREAT ANALYSIS**

a. Thorough analysis of the threat is critical to understanding the Antiterrorism/Force Protection (AT/FP) concerns. The threat analysis process results in the implementation of AT/FP plans and the allocation and expenditure of force protection resources. In addition, threat analysis provides the intelligence officer with information upon which to base warnings. ECJ2, in consultation with the DIA, embassy staffs, and applicable host-nation authorities, obtains, analyzes, and reports information specific to the USEUCOM **AOR in order for AT/FP elements to take action to protect assets.**

b. The primary sources of intelligence information for the DoD Combating Terrorism program are **government sources**, open source materials (commercial news media), criminal information, and local information.

**2. DoD THREAT ANALYSIS METHODOLOGY**

a. DoD developed a methodology to assess the terrorist threat to DoD personnel, facilities, materiel and interests. **DoD is the only user of this methodology;** other U.S. Government Departments and Agencies may apply their own analytical methodology to form their own terrorist threat analyses. This methodology does not address threats from conventional forms, i.e., hostile conventional armed forces. In addition, this methodology does not address the criminal threat (if unrelated to known or suspected terrorist activity). The DoD terrorism threat level assessment methodology uses all source analysis. The system is flexible and threat levels are revised as terrorism indicators, warnings and activities occur or change.

b. DoD identifies four factors to use in shaping the collection and analysis of information from all sources bearing on the terrorist threat. The factors in making terrorist threat analyses are applied on a country-by-country basis.

**(1) Operational Capability.** How dangerous are terrorists in this country?

**(2) Intentions.** How threatening are the terrorists in this country?

**(3) Activity.** What type of activity are the terrorists engaged in?

**(4) Operating Environment.** How do circumstances impede or constrain terrorist operations?

**3. TERRORISM THREAT LEVELS**

## FOR OFFICIAL USE ONLY

a. The DoD terrorist threat analysis community developed a notation system to describe the country-specific results of terrorist threat analysis based on the terrorism threat analysis methodology briefly described above. Though a **general** Terrorism Threat Level is given for each country, the actual terrorist threat in that country may vary from region to region, based on the modus operandi of existing groups.

b. DoD uses a four step scale to describe the severity of the threat as judged by intelligence analysts. These four steps from highest to lowest are:

(1) Terrorism Threat Level HIGH. Anti-US terrorist group is operationally active and uses large, casualty-producing attacks as its preferred modus operandi. There is a substantial DoD presence and the Operating Environment favors terrorists.

(2) Terrorism Threat Level SIGNIFICANT. Anti-US terrorists are operationally active and attack personnel as their preferred method of operation or a group uses large casualty-producing attacks as its preferred method but has limited operational activity. The Operating Environment is neutral.

(3) Terrorism Threat Level MODERATE Terrorists are present but there is no indication of anti-US activity (possible collateral threat). The Operating Environment favors the Host Nation/US.

(4) Terrorism Threat Level LOW. No terrorist group detected or terrorist group activity is non-threatening.

c. Terrorism Threat Levels describe the terrorist threat environment in a country or region where terrorist activity occurs with distinct definitions for each threat level. Threat levels are assigned based on analyzing available intelligence.

d. Terrorism Threat Levels do not specify a given Force Protection Condition. Terrorism Threat Levels do not allocate protective resources. Threat Levels do not address when the terrorist attack will occur. The issuance of Terrorism Threat Levels is not a warning notice, in and of itself. Formal terrorism warning reports are issued separately (see paragraph 4b, below).

e. Changes in Terrorism Threat Level Declarations. Analysis of terrorism is an ongoing process. Although each analysis relies on information included in previous assessments, judgments with respect to threats to DoD-affiliated personnel, facilities, and assets begin anew with each analysis. No formal escalation ladder of Terrorism Threat Levels exists; Terrorism Threat Level designations for each country or region are applied on the basis of current information and analysis.

## 4. DISSEMINATION OF THREAT WARNINGS

B-2-2

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

**a.** The Threat Warning Report replaces the previous CRITICAL threat level. It is intended to expedite warning and to be treated as distinct from a threat level change. Terrorist threat warning is accomplished in DoD using two mechanisms. The Intelligence Community system issues fully coordinated Terrorist Threat Alerts and Terrorist Threat Advisories. The Services are accorded the opportunity to comment upon proposed warnings. The Services direct their responses through DIA, the agency representing the DoD in the structure. The Executive Coordinator, Community Counterterrorism Board, is responsible for coordinating threat warnings outside CONUS. The FBI is responsible for coordinating and issuing Intelligence Community warnings for threats in CONUS.

**b.** The DoD's Defense Indications and Warning System (DIWS) comprises a second, independent system in which members at any level may initiate unilateral threat warnings. These are termed Terrorism Warning Reports (TWRs). Warnings within the DoD system generally stay within the system and are primarily for use of DoD activities. DIWS Terrorist Threat Warning Reports may be prepared and issued by any member of the DIWS system.

**(1)** Individual Commands also have the right to independently notify their members of impending threats. If an intelligence activity receives information leading to an assessment of an imminent terrorist attack, it may exercise its right to issue a unilateral warning to its units, installations, or personnel identified as targets for the attack. If an intelligence activity issues a unilateral warning, it must label threat information disseminated as a unilateral judgment, and should inform DIA of its action.

**(2)** Terrorism Warnings are issued when specificity of targeting and timing exist or when analysts determine sufficient information indicates U.S. personnel, facilities, or interests, particularly those of DoD, are being targeted for attack. Terrorism Warnings need not be country specific and a warning can cover an entire region. The key to effective Terrorism Warnings is the terrorism analyst recognizing the pre-incident indicators for an attack are present (see also Annex B, Appendix 4, BLUE DART Program).

**(3)** DIWS Terrorism Warning Reports are specific products. They are unambiguous--it is clear to the recipients they are being warned. Warnings are intended for distribution up, down, and laterally through the chain of command--not just downward. Warnings of impending terrorist activity are likely to have national implications and will be provided routinely to decision makers at the policy level of the U.S. Government.

**5. HOST NATION/NATO INTELLIGENCE SHARING.** Whenever possible, intelligence producers must consider user needs. Many installations/activities work closely with their Host Nation counterparts either as the primary or secondary means of installation/activity security. In addition, a number of installations/activities are home to combined operations or headquarters, such as NATO or even the UN.

**B-2-3****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

a. Whenever possible, intelligence and threat warning producers should classify material to allow for use by the Host Nation or NATO (e.g., SECRET-REL NATO, or SECRET-REL UK/GE/IT). Providing unclassified tear lines to share as much of the threat data as possible will also increase interoperability as we address the security risk.

b. Intelligence consumers. If a document is marked SECRET, unless something exists allowing release through the Foreign Disclosure process, only US access is authorized. If it is releasable to another country or NATO, the appropriate markings would have to be applied in order to properly release it. If not so marked and you have a need to release the intelligence outside of U.S. channels, you must go to the originator of the information to determine whether it can be released.

**6. DEPARTMENT OF STATE (DOS) THREAT ASSESSMENTS AND THREAT LEVELS**

a. DOS publishes an important series of **useful** threat assessments to DoD AT/FP program managers, but should not be confused with the assessments and Terrorism Threat Levels resulting from the DoD Threat Analysis methodology.

b. Under the provisions of the Diplomatic Security Act of 1986, 22 USC 4804 (4), the Bureau of Diplomatic Security (DS) has specific statutory responsibility and authority for conducting threat analysis programs on behalf of DOS. As part of these ongoing programs DS updates and publishes on a semiannual basis a Security Environment Threat List (SETL) reflecting Threat levels for all active Foreign Service posts permanently staffed by direct-hire U.S. personnel and non-Combatant Command U.S. military elements, operating under the authority of a Chief of Mission (COM). The SETL may also reflect threat levels for some select foreign service Posts where operations have been temporary suspended or closed, but where threat levels continue to be relative to certain DS programs.

c. The DOS threat assessment process evaluates all-source information relative to six broad threat categories, then determines corresponding threat levels. Each of the six categories is assigned a threat level for a specific post. The following describes the DOS threat categories and reflects the appropriate classification level when the designated threat level is associated with a specific Post (or Posts by name):

(1) Transnational Terrorism. Sensitive But Unclassified (SBU)

(2) Indigenous Terrorism. Sensitive But Unclassified (SBU)

(3) Political violence (includes inter-state war, civil war, coups, civil disorder and insurgency). Sensitive But Unclassified (SBU)

**FOR OFFICIAL USE ONLY**

(4) Counterintelligence (the HUMINT threat posed by hostile intelligence services). SECRET/NOFORN (S/NF)

(5) Technical (the threat posed by anti-U.S. technical intelligence activities). SECRET/NOFORN (S/NF)

(4) Crime (the residential crime environment affecting the official U.S. community). Unclassified (U)

NOTE: "SBU" is equivalent to, and should be handled as For Official Use Only (FOUO) within DoD channels.

d. DOS threat levels (from lowest to highest) are "NO DATA," "LOW," "MEDIUM," "HIGH," AND "CRITICAL." (No Data is reflected when there is no reporting of threat data from a Post, or the Post is closed.)

e. SETL Threat Levels coupled with a Post's physical security vulnerabilities serve to aid DS management in prioritizing overseas security programs and ensuring the effective allocation of resources that are applied to OSPB Overseas Security Policy Board) interagency coordinated Standards.

(1) The SETL reflects an evaluation of threat levels for a particular period of time, and these levels may be raised or lowered during scheduled reviews as situations change. The SETL does not attempt to reflect the day-to-day security environment of a given locality, but rather is intended to provide a longer-term picture for planning and resource allocation (force protection) purposes.

(2) DOS has the capability to immediately warn personnel under COM authority of specific terrorist threats. In instances when DOS/DS deems threat information to warrant an immediate response, DOS will commit security resources as necessary to deal with particular situations, regardless of the assigned SETL threat levels.

(3) DOS threat levels are the result of post inputs and coordination within Diplomatic Security, DOS, and other USG agencies at the national level (exactly which agencies are consulted varies according to the threat category). However, as the SETL is intended to assist DOS/Diplomatic Security for planning and operational purposes, the final arbiter for disputed threat levels is the Director of Diplomatic Security.

7. **"NO DOUBLE STANDARD."** The U.S. Government has adopted a policy of "No Double Standard." Terrorist threat warning may not be issued solely to personnel in the U.S. Government if the general public is included in, or can be construed to be part of, terrorist targeting. Terrorist threat warnings may be issued exclusively within government channels only when the threat is exclusively to government targets. The Department of State is the sole approving authority for releasing terrorist threat information to the public.

**FOR OFFICIAL USE ONLY**

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
**General, USAF**

**B-2-6**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****APPENDIX 3 (COUNTERINTELLIGENCE) TO ANNEX B (INTELLIGENCE) TO  
USCINCEUR AT/FP OPOD 01-01**

**1. SITUATION.** The nature of the USEUCOM mission and the resulting disposition of USEUCOM forces and facilities throughout the AOR places U.S. personnel, installations and activities at risk to attack from terrorist, criminal, subversive, foreign intelligence extremist, and other groups who target US interests for political or ideological reasons. Deliberate damage to USEUCOM facilities or operations or injury or death to USEUCOM personnel can occur primarily in two manners: (1) as the result of direct targeting or (2) as the result of "being in the wrong place at the wrong time." While the vast majority of USEUCOM forces are permanently land based in the United Kingdom, Germany, Italy, and Turkey, small numbers of U.S. Military personnel and their families provide support at U.S. Embassies and other locations throughout the AOR. An increasing problem is the threat to in-transit forces, defined as those forces occupying an area for 24-72 hours where there are no established U.S. facilities. Due to potentially volatile situations within the theater, the establishment and deployment of Task Forces (TF), Joint Task Forces (JTF) and Combined Task Forces (CTF) are common occurrences. Additionally, USEUCOM personnel routinely perform military missions such as training, military to military exchanges, assistance visits, port calls, and other special activities throughout the AOR, often away from fixed U.S. military installations. Travel during official temporary duty or leave may also place U.S. military personnel (and their families) away from security normally afforded by fixed military installations. USEUCOM's high level of operational activity combined with the asymmetric nature of force protection threats creates a highly volatile and unpredictable environment. As a result it is essential to be able to obtain timely, relevant information regarding threats to USEUCOM forces and facilities to ensure appropriate and responsive countermeasures are taken. A key consideration in USEUCOM's ability to obtain such timely focused information is the effective placement and use of limited Counterintelligence (CI) resources. Proper placement of CI assets can assist in obtaining this information, thereby aiding in efforts to mitigate force protection threats to an acceptable level. The terrorist threat is asymmetric in nature; there is no protected border. Thus, the USEUCOM perspective is that placement and use of CI assets should be determined based upon an analytical determination of threat activity in relation to the nature and degree of friendly force presence and/or activities.

**2. MISSION.** Conduct counterintelligence operations, investigations, collection, liaison and other activities throughout the USEUCOM AOR in peacetime, crisis or hostilities in order to identify, neutralize and defeat threats to USEUCOM forces and facilities from foreign intelligence security services (FISS), state sponsored terrorist groups, militant extremists and other groups who target U.S. personnel, installations, or activities.

**3. EXECUTION**

**a. Scheme of support.** CI Support within USEUCOM is provided by the USAF Office of Special Investigations (AFOSI), the Naval Criminal Investigative Service (NCIS), and Headquarters Department of the Army (HQDA) counterintelligence

**FOR OFFICIAL USE ONLY**

organizations. In peacetime USCINCEUR has no direct tasking authority of AFOSI or NCIS; however, AFOSI and NCIS conduct counterintelligence activities consistent with the USEUCOM CI Strategy and USCINCEUR theater engagement strategy. Thus, service CI component assets will be employed in a coordinated fashion to support the USEUCOM Antiterrorism/Force Protection (AT/FP) mission:

**(1)** US Army Europe (USAREUR): The 66<sup>th</sup> Military Intelligence Group and V Corps' 205<sup>th</sup> MI Brigade, and USAREUR Office of Deputy Chief of Staff, Intelligence (ODCSINT) Federal/National level liaison officers (Theater Support Representatives (TSRs and/or MLO-Military Liaison Officers) provide CI support to USAREUR and the theater.

**(2)** US Air Forces in Europe (USAFE): The US Air Force Office of Special Investigations, 5<sup>th</sup> Field Investigations Region, a Service CI organization, provides CI support to USAFE and the theater.

**(3)** US Naval Forces, Europe (USNAVEUR) and Marine Forces Europe (MARFOREUR): The NCIS European Field Office provides CI support to USNAVEUR and MARFOREUR, and the theater.

**b. Tasks to subordinate units**

**(1)** Using organic (assigned and attached) assets, component CI commands and CI elements operating in support of USEUCOM established TFs, JTFs and CTFs will:

**(a)** Conduct Counterintelligence Operations and activities in accordance with the current USEUCOM Theater Counterintelligence Strategy in order to identify, neutralize and defeat threats to USEUCOM forces and facilities.

**(b)** Collect, process, and disseminate timely, accurate, and relevant information on terrorists and other individuals or groups (criminal, subversive, foreign intelligence and security services (FISS), extremist groups who oppose US Policy or presence) whose interests are inimical to US personnel, installations, or activities. The goal is to provide commanders warning of possible attacks, providing time, place and method so as to assist them in making decisions on protecting personnel, installations, activities and material.

**(c)** Provide CI threat/vulnerability assessments as part of physical and operational security (OPSEC) assistance programs, training, exercises, and as part of deployment preparation, in response to supported commanders' requests.

**(d)** Actively participate in physical and operational security (OPSEC) assistance programs, in response to supported commanders' requests and within capabilities.



**FOR OFFICIAL USE ONLY**

- (e) Assist with supported commanders' security education programs by:
  - (1) Providing training/briefings on threats posed by FISS, terrorists, criminals (if appropriate), subversives, extremist groups and others whose interests are inimical to US personnel, installations, or activities.
  - (2) Providing training/briefings on espionage, sabotage, and subversion techniques likely to be encountered.
  - (3) Providing foreign travel briefings tailored to individual unit needs and circumstances.
  
- (f) Advise supported commanders on the availability and appropriateness of CI technical services.

**(2) HQ USEUCOM**

- (a) **USEUCOM Counterintelligence Support Officer (CISO).** The CISO is specifically responsible for:
  - (1) Advising ECJ2, ECSM, and DCINCEUR/USCINCEUR on significant CI investigations, operations, collections, and production activities affecting the command.
  - (2) Ensuring significant foreign intelligence threat information developed in the combatant commander's AOI is forwarded to the J2 and other principal staff officers.
  - (3) Ensuring significant foreign intelligence threat information flows from the command's components, through the command, to the joint staff, and concurrently from the command to its components.
  - (4) Coordinating CI support activities within the command's headquarters staff and among components' CI organizations.
  - (5) Coordinating with US Agencies and Country teams where appropriate and necessary to support USCINCEUR's CI requirements.
  - (6) Coordinating the tasking of CI Organizations in the command's AOR or AOI upon CJCS-approved operation plan (OPLAN) implementation, during CJCS-directed contingency operations, JTFs and CTFs, or in support of unilateral and multinational deployments and joint exercises.
  - (7) Upon **Presidential and Secretary of Defense** directed contingency operation or OPLAN execution, advise USCINCEUR during and after assumption of OPCON of supporting CI forces.
  - (8) Advising USCINCEUR on CI support to counter-drug and OPSEC programs and the combating terrorism (CbT) and antiterrorism (AT) activities within the command's AOR.
  - (9) Ensuring command's CI participation in joint planning and policy process.
  - (10) Ensuring CI is considered in the Command Intelligence Architecture Plans (CIAPS).
  - (11) Ensuring CI analytic support in the development and staffing of the JIC/JAC.

**FOR OFFICIAL USE ONLY**

(12) Ensuring CI collection and production priorities are integrated into the command's collection and production plans.

(13) Representing the command's CI interests in national-level meetings.

(14) Coordinating with ECSM representatives to ensure all CI liaison activities support the overall USEUCOM Force Protection effort. The CISO will also coordinate with ECSM representatives to obtain any special contact requirements as outlined in specific CINCEUR/Chief of Mission Memoranda of Agreement. The CISO will also provide such information to the individual CI components to ensure they are aware of particular country team requirements.

(15) Serving as the Chief of the Counterintelligence Branch, Operations Division, USEUCOM ECJ2.

(16) During crisis or contingency, overseeing/directing functions outlined in Appendix H of reference (g).

**(b) USEUCOM Counterintelligence Branch, CI Section (ECJ23-CI)**

(1) Serves as the CISO's staff and represents the Command and the CISO in matters relating to CI operations, investigations, collections, and support activities.

(2) Is responsible for CI planning, policy development, contingency support, coordination and liaison within the theater and with national level agencies.

(3) Coordinates CI operational activities among the USEUCOM staff and coordinates and deconflicts CI operations among component and Service CI elements.

(4) Provide staff subject matter expertise relating to CI and CI activities within theater.

**(c) USEUCOM Counterintelligence Branch, Combating Terrorism (CbT)**

**Section**

(1) Determine, prioritize, focus, facilitate and integrate CbT activities and operations.

(2) Serve as primary J2 focal point for terrorist threat information in support of Force Protection activities with ECSM.

(3) Coordinate CbT activities with Staff, components and partner nations.

(4) Monitor terrorist threat information and ensure dissemination to affected units.

(5) Integrate HUMINT/CI/LE assets as critical collection/targeting elements in campaign.

**(d) USEUCOM Joint Analysis Center (JAC).** Responsibility for USEUCOM CI analysis, production, and dissemination is centralized at the JAC Counterterrorism/Counterintelligence (CT/CI) Division DOX JAC/DOX has a functional Counterintelligence analytic capability. The Division produces specialized CI products

**FOR OFFICIAL USE ONLY**

in support of USEUCOM exercises, and interfaces with other JAC branches to nominate targets for exploitation, neutralization, or destruction.

(e) Component command CI elements will develop policies or programs that address the following:

(1) Develop procedures to be taken in support of supported commander's terrorist incident response plans.

(2) Coordinate CI activities supporting AT/FP plans and programs through established DoD procedures.

(3) Develop and exercise (or participate in exercises) CI support for AT/FP procedures.

(4) As appropriate and within capabilities, participate in installation physical security vulnerability assessments.

(5) As appropriate, support designated supported commanders as they annually exercise their AT/FP Plans or when the Terrorism Threat Level or Force Protection Condition changes.

(6) Within capabilities, support requested AT/FP training of deploying personnel and units.

**c. Coordinating Instructions**

(1) **Liaison.** CI liaison between USEUCOM CI Components is essential to effectively mitigate force protection threats. USEUCOM recognizes each service CI component brings individual strengths to the theater. Further, USEUCOM recognizes there are specific service equities that must be preserved and protected. In full view of these considerations, USEUCOM considers effective coordination between CI components as discussions leading to greater synergy of effort and sharing of lessons learned. CI components are encouraged to seek mechanisms where they can optimize individual component expertise (investigative, ground, air, etc) and to find ways to achieve cost savings that lead to more efficient and effective execution of the overall EUCOM CI mission. A tool to assist in maintaining effective coordination and cooperation between the CI components and the EUCOM staff is the Cooperative Agreements Working Group (CAWG). The CAWG will be used to the maximum extent feasible by the CI components and the CISO to facilitate timely and effective coordination. Components are authorized to conduct CI liaison with friendly foreign/ host nations concerning force protection in accordance with governing service directives, DIAM 58-11, DCID 5/1 and pertinent USEUCOM directives. Component CI agencies will coordinate with the CISO to obtain information regarding any special liaison requirements established between CINCEUR and a particular Chief Of Mission (COM), and/or the Defense Attaché.

(2) **Training.** Component commands will ensure adequate CI resources are appropriately trained and are available to protect against attempts of espionage, sabotage, surprise, subversion, unauthorized observation, other intelligence activities, or terrorism.

**FOR OFFICIAL USE ONLY**

(3) Supported commanders deploying outside of their host country must request threat assessments for the deployment area from their supported CI element.

(4) During normal operations (other than during the execution of CJCS-approved OPLAN, CONPLAN or OPORD) component command and supporting Service CI organizations remain under the command and control of their component and/or military service and CI organizational headquarters. USEUCOM exercises coordination authority over supporting CI components through the J2 and CISO.

(5) During the execution of CJCS-approved OPLAN, participating CI units shall come under USEUCOM's operational control through their respective component commanders, IAW applicable plans. Administrative control will remain with the component and/or CI organizations of each military service. CI elements support their Service component in theater, but may also be tasked through the CISO or TFCICA (Task Force Counterintelligence Coordinating Authority).

(6) Contact can be made with the USEUCOM CISO or the Counterintelligence Branch via the following methods:

- ❑ **STU III Telephone:** (DSN) 430-8123/7421/5761 (COMM) (49) 711-680-8123/7421/8154.
- ❑ **STU III FAX:** (DSN) 430-6982/8240 (COMM) (49) 711-680-6982/8240.
- ❑ **Unsecure FAX:** (DSN) 430-6344. (COMM) (49) 711-680-6344.
- ❑ **SLAN/SIPRNET address:** "J2-CI@eucom.smil.mil".
- ❑ **GENSER ADDRESS:** USCINCEUR INTEL VAIHINGEN GE//ECJ23-CI//.
- ❑ **SSO ADDRESS:** USEUCOM//ECJ2-SSO/ECJ2-CI//.

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
**General, USAF**

**FOR OFFICIAL USE ONLY****APPENDIX 4 (BLUE DART PROGRAM) TO ANNEX B (INTELLIGENCE) TO  
USCINCEUR AT/FP OPOD 01-01****1. GENERAL**

a. BLUE DART is an Antiterrorism/Force Protection (AT/FP) threat-warning program designed to rapidly disseminate threat information as fast as possible directly to affected areas and units in a simple, easy to understand format. The program covers all USEUCOM subordinate and tenant units as well as other official, U.S. sponsored organizations in the AOR. The program also applies to NATO and allied units operating under U.S. auspices and other non-military U.S. organizations including U.S. embassies. BLUE DART is a command-wide program, and dissemination of BLUE DART warning messages will not be limited to intelligence channels.

b. Any unit or entity covered by the program can initiate a BLUE DART. Because BLUE DART warnings are designed to provide actionable, time-critical warning to threatened units, USEUCOM developed a specific set of criteria information must meet in order to be issued as a BLUE DART. This information must contain a specific threatened location, unit, and means of threat and must be applicable within a specific near-time frame. Specificity is the key principle of this program. If information cannot be used to provide specific, actionable warning, it will not be treated as a BLUE DART. However, in order to ensure timely warning, information included in a BLUE DART does not need to be validated or confirmed before transmission. This approach may result in the passing of some erroneous information, but some false reporting is accepted in order to ensure timely warning of specific threats.

c. BLUE DART requires two forms of notification. Immediate voice notification by telephone or radio directly to the targeted unit or installation ensures threat information is passed by the fastest means possible and provides immediate feedback from the receiving unit, thereby confirming its reception and interpretation. Follow-up notification is then accomplished through appropriate message handling systems. According to USEUCOM guidelines, initial voice notification must be completed within 10 minutes of threat information reception. Throughout repeated exercises and numerous real-world situations, USEUCOM has demonstrated the ability to meet this timeline and averages approximately 2 minutes.

d. HQ USEUCOM ECJ23 Intelligence Operations Center (IOC) exercises overall staff proponent for the BLUE DART program in coordination with ECSM. The IOC is responsible for implementing BLUE DART warnings, conducting quarterly tests of the system, and providing feedback to ECJ23 to establish and adjust the theater-wide threat warning policy for all systems (to include BLUE DART). ECSM is responsible for providing guidance regarding prescriptive measures for reacting to BLUE DART and other threat warnings.

**e. Scope of Program**

B-4-1

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

(1) BLUE DART applies to real world and BLUE DART exercise imminent threat warning.

(2) Broadcast of BLUE DART reports is preferred for widest dissemination.

(3) Priority should be given to the threatened unit(s) **within 10 minutes** of receipt of the initial warning information.

(4) Immediate up-and cross-echelon reporting is required to ensure commanders have information on which to base guidance and assistance to threatened subordinate units.

(5) In general, BLUE DART messages should not be held while information contained in them is verified. Some false alarms may be reported without this verification; nevertheless, some level of false reporting is accepted to guarantee rapid reporting.

(6) Feedback is requested both on real-world and exercise messages.

(7) Imminent threat warning reports not containing the words "BLUE DART" but meeting BLUE DART reporting criteria should be disseminated immediately as BLUE DART warning reports.

(8) 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 reported as a BLUE DART unless an incident suggests follow-on threats are likely and imminent.

(9) Any unit in receipt of information meeting BLUE DART criteria is required to immediately initiate a BLUE DART warning report.

**(10) Examples:**

(a) A threat report with a specific threatened location (e.g., Tuzla AB), a specific threatened unit (e.g., TF Eagle), a specific threat means (e.g., car bomb attack against checkpoint) within a specific near-term time frame (e.g., at 2300z, or within the next two hours) or some combination of these normally would be reported as BLUE DART.

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

**FOR OFFICIAL USE ONLY**

(c) 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 are about to follow.

(d) Examples of what should or should not be a BLUE DART cannot be all-inclusive. Ultimately, we must rely on the judgment of our watch standers, analysts and operators. Over-use of the term BLUE DART will diminish its usefulness as a means of imminent threat warning; however, when in doubt, erring on the side of using the term BLUE DART is recommended. Terrorism threat warning not meeting BLUE DART criteria will be disseminated IAW normal procedures.

**2. EXECUTION****a. Threat Dissemination**

(1) **Initial Warning.** BLUE DART warnings will be passed to the targeted unit by the fastest means possible. Unclassified communications may be used but only when non-secure means are unavailable or judged too slow. Component intelligence organizations and deployed task forces will establish written procedures to ensure timely introduction of BLUE DART threat warning to command and control nets while continuing to relay information via intelligence nets. Operational organizations will execute BLUE DART procedures and inform supporting intelligence organizations when they identify threat information meeting BLUE DART criteria. This allows further dissemination of information and provides focused intelligence support to the problem.

(2) **Subsequent Reports.** After initial voice notification to the targeted unit, the organization originating a BLUE DART will follow-up with FLASH precedence record message traffic up its chain to HQ USEUCOM, including JAC Molesworth, and all pertinent theater component watches and intelligence elements.

**b. Installation and Unit Procedures.** Each command with access to communications is responsible for establishing local procedures and watch standards for passing BLUE DART threat warning information. Procedures will address dissemination to lower, adjacent, and higher units.

**c. Command Center Procedures.** Tactical and fixed command centers at all levels are responsible for creating or modifying local procedures and training watch standers to carry out BLUE DART guidance. Command Centers at all echelons will maintain the capability to execute BLUE DART warnings and have checklists in place to facilitate the rapid dissemination of BLUE DART messages. Imminent threat warning information must be passed immediately up, down and cross-echelon on assigned command nets. The first priority is to the threatened unit(s); however, reports must be passed up and cross-echelon as well as down-echelon to ensure responsible commanders and headquarters have information on which to base further guidance and assistance.

**FOR OFFICIAL USE ONLY**

**d. 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 **10 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 by the most expedient secure means where immediately available, or by the most expedient means when secure means are not immediately available.

**e. Redundant Communications.** Voice and message dissemination are necessary to ensure timely delivery of imminent threat warning information. Follow-up initial reporting with hard copy (record message, e-mail or fax) messages when BLUE DART warning is carried out via a voice. Send voice reports to follow-up and to confirm receipt of initial reporting when ~~is~~ carried out via message, e-mail, or data link, such as a voice alert upon receipt of TIBS or TDDS information displaying the location of a specific threat. Use broadcast wherever possible to ensure widest dissemination in the shortest time.

**3. ADMINISTRATION AND LOGISTICS.** Commanders are responsible for immediately informing USCINCEUR, via the chain-of-command, of equipment or procedural shortfalls that would prevent execution of provisions of this guidance.

**4. COMMAND AND CONTROL.** Secure telephone or secure radio, if available, will be used for the immediate voice notification. If a secure means is not available then non-secure telephone or radio may be used. The follow up will be sent via hard copy message.

**5. BLUE DART EXERCISE PROCEDURES**

**a.** HQ USEUCOM ECJ23 Intelligence Operations Center (IOC) Watch will exercise BLUE DART procedures **quarterly** to maintain awareness and proficiency. **Theater exercise** messages will be sent only with the express permission of HQ USEUCOM IOC, who will coordinate the action with other appropriate staff elements, e.g., ECJ3-ETCC, ECSM, etc. **The IOC will identify an exercise OPR to initiate the theater exercise by originating a message from a** field unit, headquarters, or supporting intelligence center in or out of theater. Test considerations are as follows:

(1) Exercise messages will be sent from a variety of locations based on **notional** intelligence collection from different sources (HUMINT, IMINT, SIGINT, etc.).

(2) Exercise messages are intended to be received by a variety of units to ensure circuits and procedures function properly.



**FOR OFFICIAL USE ONLY**

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

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

b. Immediately acknowledge receipt of the BLUE DART message to the sender. The ultimate recipient of the warning will report back to USEUCOM headquarters within two hours the time received, from whom, and by what means. Report back by SIPRNET to [j2watch@eucom.smil.mil](mailto:j2watch@eucom.smil.mil), SCI e-mail to [USEUCOM\\_IOC@hq.eucom.ic.gov](mailto:USEUCOM_IOC@hq.eucom.ic.gov), via Coastline TAN ISSO or ISSP, or message to HQ USEUCOM VAIHINGEN GE//ECJ23/ECJ23-IOC/ETCC// with information copy to HQ USEUCOM VAIHINGEN GE //ECJ2/ECJ3/ECJ6/ECSM//. Provide information copies to others in chain of command as necessary. If unable to report by message or e-mail within 2 hours, report by phone (DSN 430-8132/8135; COM 49-711-680-8132/8135) or LOCE phone (030), or relay to unit with this capability. Other commands/units in receipt of BLUE DART exercise traffic will report this same information by routine message within 24 hours to HQ USEUCOM VAIHINGEN GE//ECJ23-IOC/ETCC//, with information copy to HQ USEUCOM VAIHINGEN GE//ECJ23-CI/ECSM/ECJ3// and JAC MOLESWORTH RAF MOLESWORTH UK//DO/DOAT/JOC//. Provide comments if desired (for JAC at DSN 268-2235 or JAC/DOAT 268-1510).

c. If an exercise BLUE DART interferes with a real-world BLUE DART or other time-critical threat warning, any unit involved is authorized to terminate the BLUE DART exercise. To terminate an exercise, report the following by all appropriate means: quote "terminate exercise BLUE DART" unquote, and repeat the call. All units involved in the exercise report back to USEUCOM headquarters as described in paragraph c, above, the information collected up to exercise termination. The unit terminating the exercise is also to provide the reason for exercise termination.

d. Example exercise message:

```
FM/TO:
EXERCISE     EXERCISE     EXERCISE
(U) SUBJ: EXERCISE BLUE DART XXX-99
PASS THIS EXERCISE MESSAGE TO:(...)
EXERCISE     EXERCISE     EXERCISE
```

e. Component and other theater units may initiate internal threat notification exercises as part of their training programs. However, only the IOC may initiate or approve a Blue Dart exercise due to the required coordination to involve Theater resources. If a component or other subordinate theater unit wishes to conduct a Blue Dart exercise, they must coordinate it with the IOC and receive the IOC's approval a minimum of two weeks before conducting the exercise.

**FOR OFFICIAL USE ONLY**

6. There should never be confusion about whether a BLUE DART is real or an exercise. Four things distinguish the exercise message from the real-world one: (a) "Exercise BLUE DART" in the subject line; (b) an exercise number in the subject line; (c) the word "exercise" three times before and three times after the text; and (d) only passing instructions in the text -- no scenario. A real-world BLUE DART contains a specific threat. Additional words in the subject line or message such as "tipper" or "warning" do not change the fact that the message is a real-world BLUE DART.
7. To date it is unproven BLUE DART reports have prevented any casualties. However, the program is having the intended consequences. Service members stop what they are doing and pay attention, because taking immediate action might save a life. A single instance of this program's prevention of a death or injury will be worth all the effort put forth to implement this program. Force protection remains our priority.

**ACKNOWLEDGE:**

**JOSEPH W. RALSTON**  
**General, USAF**

**FOR OFFICIAL USE ONLY**

**APPENDIX 5 (THEATER TERRORIST THREAT ASSESSMENT) TO ANNEX B  
(INTELLIGENCE) TO USCINCEUR AT/FP OPOD 01-01**

The substance of this Appendix is classified at the Secret level and can be found on the USEUCOM Joint Analysis Center (JAC) homepage on the SIPRnet INTELINK-S at <http://www.jac.eucom.smil.mil/> with additional information derived from more sensitive intelligence sources and methods available on the JAC homepage on Joint Worldwide Intelligence Communications System (JWICS) INTELINK at <http://www.jac.eucom.ic.gov/>.

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
**General, USAF**

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**B-5-2**  
**FOR OFFICIAL USE ONLY**

# FOR OFFICIAL USE ONLY

## ANNEX C (OPERATIONS) TO USCINCEUR AT/FP OPORD 01-01

### REFERENCES: See Basic Order

**1. SITUATION.** The geographic area of operations (AO) encompassed by this order includes the land, sea, and airspace of the USEUCOM AOR. Key AT/FP program elements required for aggressive and effective AT/FP operations include the following: the Terrorism Threat Assessment and Vulnerability Assessment to include both conventional and weapons of mass destruction (WMD); Risk Management in mission planning and execution as well as installation/facility protection; Force Protection Conditions (formerly known as THREATCON) keyed to the local environment; Terrorist Incident Response Measures to include WMD; procedures for Force Protection Condition transition; and Consequence Management Measures to mitigate effects of a terrorist attack.

**2. MISSION.** To provide policy and guidance for the execution and oversight of USCINCEUR's AT/FP program. To outline the operational requirements, procedures and standards for the USEUCOM AT/FP program.

### 3. EXECUTION

**a. Scheme of Support.** The foundation for an effective AT/FP program and AT/FP readiness is the development of a comprehensive plan. Commanders at all levels shall publish and exercise such a plan to ensure that it is executable and to identify further program enhancements. Minimum AT/FP plan content and requirements include those key program elements listed in paragraph 1, above.

#### **b. Tasks to subordinate units**

**(1)** Service component commander responsibilities are as specified in the basic order.

**(2) HQ USEUCOM ECSM.** Act as the primary focal point for AT/FP for USCINCEUR. ECSM, using its coordinating authority, shall:

**(a)** Establish command policies and programs for the protection of DoD personnel and their families, facilities, and material resources from terrorist acts, as required by DoDD 2000.12, reference (g).

**(b)** Monitor and assist Service component and subordinate commanders, Defense Agencies, and other DoD elements and personnel for whom the CINC exercises TACON (for force protection) within the USEUCOM AOR, with implementation of the AT/FP program requirements specified in DoDI 2000.16, reference (j).

## FOR OFFICIAL USE ONLY

**(c)** In coordination with ECJ3 and/or ECJ5, identify and disseminate to force providers area specific pre-deployment training requirements which all units must complete prior to arrival in theater. Provide AT/FP training requirements to the Services and Defense Agencies for all DoD personnel and families scheduled for permanent change of station to or within the theater. Ensure all personnel assigned to USEUCOM headquarters receive appropriate AT/FP training.

**(d)** Monitor DoD Terrorism Threat Levels, Defense Terrorism Warning Reports and Force Protection Conditions throughout the AOR. Ensure Force Protection Conditions are uniformly implemented and disseminated. Coordinate and de-conflict Force Protection Conditions set by subordinate commands when required.

**(e)** Provide a representative to the DoD Antiterrorism Coordinating Committee and Subcommittees, as required, and to the DoD Worldwide Antiterrorism Conference.

**(f)** Validate AT/FP resource allocation requests, submitting prioritized recommendations to the USEUCOM Comptroller (ECCM) for budget process implementation.

**(g)** Monitor dissemination of AT/FP information, to include emerging advanced technologies, within the USEUCOM AOR.

**(h)** Actively seek additional means and initiatives to improve USEUCOM AT/FP processes and programs.

**(i)** Act as principal point of contact for AT/FP issues and requirements tasked by higher authority.

**(j)** Act as the AT/FP proponent at key forums such as the Component Commanders Conference (CCC), the CJCS CINCs' Conference and the JROC. These are ideal forums to highlight AT/FP issues and concerns. Additionally, ECSM is the proponent for several command specific AT/FP forums:

**(1)** Staff proponent for the General/Flag Officer Antiterrorism Steering Group (GOASG). See Annex C, Appendix 5, Tab A.

**(2)** Chair the USEUCOM Joint Antiterrorism Working Group (JAWG). See Annex C, Appendix 5, Tab B.

**(3)** Chair the Antiterrorism Staff Action Working Group (ASAWG). See Annex C, Appendix 5, Tab C.

**(k)** Act as USCINCEUR's troubleshooter to solve AT/FP problems, particularly time sensitive issues.

**(l)** Provide a coordination link for the Service component commands and/or local activities to work AT/FP issues with USDRs and HQ USEUCOM staff.

## FOR OFFICIAL USE ONLY

(1) Provide expertise/guidance for AT/FP issues related to the planning and execution of USEUCOM level exercises.

(2) Coordinate AT/FP for contingency deployments, with particular attention to AT/FP planning for Aerial Ports of Debarkation (APOD) and Surface Ports of Debarkation (SPOD). See Annex E.

(3) Assist Commander-In-Chief, United States Naval Forces, Europe (CINCUSNAVEUR) in assessing AT/FP requirements for port visits. Where applicable, ensure the USDR's local threat assessment is included in the planning process. See Annex E.

(m) Ensure implementation and enforcement of DoD and USEUCOM AT/FP policies, directives, and standards. This will be accomplished during AT/FP program reviews of the Service component command headquarters at least annually. This also may require spot checks, in coordination with the USEUCOM Inspector General (ECIG), for unit pre-deployment AT/FP training and equipment requirements.

(n) In coordination with ECJ5, and ECJ4 in Turkey, act as interface on AT/FP issues with the USDRs, to streamline the process, by providing them a single point of contact. This is particularly important for coordination of host nation support for AT/FP.

(o) Consolidate resource requests from Service component commanders and USDRs that require USEUCOM, Joint Staff, DoD, or interagency attention for resolution. Coordinate with the Joint Staff, ECJA, ECCM, and ECJ4 to properly earmark such requests as being AT/FP requirements.

(p) Collate theater wide AT/FP shortcomings and deficiencies for submission to the Joint Monthly Readiness Review (JMRR) and the Joint Warfighting Capabilities Assessment (JWCA).

(q) Coordinate with the Service component commands to ensure any pending housing and real property purchases are reviewed for AT/FP acceptability (see Annex D, Appendix 1). When applicable, ensure coordination with the COM to comply with statutory requirements.

(r) Develop, coordinate, and execute a CINC/COM MOA delineating AT/FP responsibilities for all DoD elements and personnel in a given country.

(s) Be responsible for oversight and coordination of AT/FP training requirements in theater. Monitor accomplishment of AT/FP training requirements in theater.

(t) Coordinate AT/FP OPSEC related matters with ECJ3, the USEUCOM proponent for OPSEC.

**(3) HQ USEUCOM ECJ1**

## FOR OFFICIAL USE ONLY

(a) Plan, task, and monitor the Service component command sourcing of AT/FP augmentation.

(b) In coordination with the 6<sup>th</sup> Area Support Group (ASG), ensure all personnel who PCS or are TDY to HQ USEUCOM receive Level I AT/FP training during in-processing, as required.

(c) In coordination with the Service component command Personnel Directorates, ensure all PCS and TDY orders for personnel stationed in USEUCOM indicate the requirement for Level I AT/FP training.

(d) Require theater clearance approvals and TDY orders to specify the authority responsible for security, either USCINCEUR or the appropriate COM, for personnel TDY within the theater.

### (4) HQ USEUCOM ECJ2

(a) Collect, analyze, and disseminate terrorist threat information for the AOR according to current DoD directives.

(1) Collect and disseminate Defense Indications and Warning System (DWIS) Terrorism Warning Reports.

(2) Collect and disseminate Intelligence Community Terrorist Threat Alerts and Terrorist Threat Advisories.

(3) Based on intelligence or information received by USEUCOM assigned or controlled intelligence activities, provide recommendations to ECSM on the issuance of unilateral terrorist threat warnings to DoD personnel in USEUCOM.

(4) Act as proponent for the USEUCOM BLUE DART Program. See Annex B, Appendix 4.

(b) Provide counterintelligence (CI) and terrorist threat assessments for the USEUCOM AOR. Use the DoD Threat Analysis Methodology to assess the terrorist threat.

(c) Provide copies of threat assessments to the Military Services, Service component commanders, JTF/CTF commanders, USDRs, COMs, and other DoD or non-DoD agencies as appropriate.

(d) Issue Defense Terrorism Warning Reports when the situation dictates. Coordinate with DIA to determine Defense Terrorism Threat Levels in the EUCOM AOR.

(e) Provide ECSM the requisite expertise on and interface to CI programs that impact AT/FP efforts.



## FOR OFFICIAL USE ONLY

(f) As required, assist ECSM in the conduct of the intelligence and/or counterintelligence portions of USEUCOM conducted Vulnerability Assessments, AT/FP Program Reviews, and/or EUCOM Survey and Assessment Team (ESAT) missions.

(g) Develop threat assessments to include estimates for potential terrorist use of WMD in the USEUCOM AOR. Immediately process and disseminate any reports of significant information obtained which identifies organizations with WMD capabilities operating in the USEUCOM AOR.

### (5) HQ USEUCOM ECJ3

(a) Determine and maintain USEUCOM Operations Security (OPSEC) Critical Information Essential Element of Friendly Information (EEFI), and publish EEFI within in EUCOM AOR in accordance with CJCSI 3213.01, reference (v).

(b) Provide OPSEC guidance to support AT/FP planning and policy development.

(c) In coordination with ECSM, ensure AT/FP guidance and requirements are included in all crisis action/operations/contingency plans and orders.

(d) In coordination with ECSO, prepare a Terrorist Incident Contingency Plan for USEUCOM.

(e) If deployed, ensure ESAT surveys include and highlight AT/FP requirements in the assessment.

(f) Coordinate and execute USEUCOM responses to any terrorist incident. During the initial stages of a terrorist incident response, the European Theater Command Center (ETCC) serves as the focal point for emergency reporting, decision making and conferences. At some point during the response phase, the ECJ3 may direct the formation of the Crisis Action Team (CAT) or a Crisis Response Cell. In either case, these teams or cells will operate out of the ETCC and act as the focal points for directing and coordinating USEUCOM crisis responses. In all cases, coordinate the initial response actions with ECSM, ECJ2 and ECSO.

(g) Keep ECSM, ECSO, ECJ2 and other affected staff members informed of any AT/FP related information received, such as Force Protection Condition changes or terrorist threat warnings, and/or reports of terrorist related activities/incidents.

(h) Ensure AT/FP tasks are included in all USEUCOM-level exercises.

(i) In coordination with ECSM, ensure AT/FP issues are included in USEUCOM's input to the Joint Monthly Readiness Review (JMRR).

C-5

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

### **(6) HQ USEUCOM ECJ4**

**(a)** Provide expertise on, and interface with, security assistance organizations and activities.

**(b)** Coordinate strategic airlift requirements and engineering support. Assist in the evaluation of designated air/seaports of embarkation in the event of non-combatant execution operations (NEO).

**(c)** Act as the proponent for the AT/FP Design Standards (see Annex D, Appendix 1 and Annex M, Appendix 1). Review and provide recommendations for approval or disapproval of all requests for deviations from the specified construction design standards.

### **(7) HQ USEUCOM ECJ5**

**(a)** Evaluate the impact of AT/FP requirements and issues on the deliberate planning process and operations/contingency plans under the cognizance of ECJ5.

**(b)** Provide expertise regarding NEO planning and execution.

**(c)** Evaluate political-military impact of AT/FP requirements and issues.

**(d)** Act as the HQ USEUCOM Office of Primary Responsibility (OPR) for administering the USDR program. Coordinate all issues involving the USDR and impacting on AT/FP with ECSM.

**(e)** Act as the HQ USEUCOM OPR for chemical, biological, and radiological issues. Provide expertise and coordinate issues dealing with WMD. Act as the proponent for the USEUCOM WMD program and the guidance issued in Annex C, Appendix 3.

**(f)** In coordination with ECSM, ensure AT/FP issues are included as part of the USEUCOM input to both the Joint Warfighting Capabilities Assessment (JWCA) and the Joint Requirements Oversight Council (JROC).

**(8) HQ USEUCOM ECJ6.** Act as proponent for AT/FP related Information Assurance. See Annex K.

### **(9) HQ USEUCOM ECJA**

**(a)** Provide expertise regarding legal issues that impact on the planning and execution of USEUCOM AT/FP program.

## FOR OFFICIAL USE ONLY

(b) Review each country-specific MOA to be signed by USCINCEUR and a COM pursuant to the DoD/DOS Universal MOU for legal sufficiency.

(c) Review all proposed changes to existing CINC-COM MOAs, to include withdrawal from an MOA by either party, for legal sufficiency.

(d) Provide legal opinion as necessary on all disputes concerning command relationships.

(e) Review any proposals to augment the JCS Standing Rules of Engagement (SROE).

(f) Review all requests and proposals for the use of CJCS Combating Terrorism Readiness Initiative Funds (CbTRIF) before such proposals are submitted to DCINCEUR for approval and forwarding to the Joint Staff.

**(10) HQ USEUCOM ECIG.** Conduct assessments and inspections of the USEUCOM AT/FP program from a systemic procedural perspective. Examine areas of AT/FP during all inspections as a USCINCEUR Special Interest Item.

**(11) U.S. Defense Representative (USDR).** Act as the senior officer responsible for the coordination of AT/FP issues for DoD elements and personnel under security authority of the COM. Serve as the primary conduit between the CINC and the COM for all AT/FP matters. Duties specifically related to AT/FP are addressed in Annex C, Appendix 4.

**(12) All CINCs, Services and Defense Agencies** providing forces to USCINCEUR or deploying forces within or through the USEUCOM AOR should coordinate all such deployments or assignments with USEUCOM to enable these forces to comply with USCINCEUR AT/FP requirements. This includes pre-deployment AT/FP planning and training for exercises and contingencies (see Annex C, Appendix 1), and JCS OPREP reporting. Supporting forces such as USTRANSCOM components that deploy to set up APODs or SPODs, or Defense Agencies and commands that traditionally remain “stove piped” to their parent command after deployment, such as the Corps of Engineers, should follow the AT/FP instructions in this order. USEUCOM will work closely with all planners to ensure the implementation of appropriate and compatible AT/FP measures.

**(13)** Nothing in this order relieves the unit or element commander of his/her inherent responsibility for the protection of assigned unit personnel. Deployed unit and element commanders shall use their normal chain of command for reporting AT/FP incidents or issues. Submit all resource, manpower and other requests for assistance through normal Service channels for execution, with information copies to ECSM when appropriate for monitoring and tracking purposes.

## FOR OFFICIAL USE ONLY

### c. Coordinating Instructions.

**(1) Deployments.** Prior to deployment of any kind to the USEUCOM AOR, all units and elements must complete and coordinate an AT/FP plan for the operation. Pre-deployment AT/FP awareness training is mandatory for all deploying personnel. Annex C, Appendix 1, Tab A lists training requirements as well as the minimum equipment requirements for deployments within the AOR. Subordinate commanders must report any deviations up their chain of command. Service component commands, JTF/CTFs, DRUs, and USDRs must coordinate all requests for deviation from AT/FP standards and seek approval from HQ USEUCOM. See Annex M, Appendix 1 for details concerning deviations (exceptions, waivers, and variances).

**(2)** All units and activities must routinely review the effectiveness of their daily physical security measures under the existing baseline Force Protection Condition and their capability to transition to higher Force Protection Conditions. Commanders at all levels must be prepared to implement requirements contained in this OPORD to achieve a higher state of AT/FP readiness when necessary.

**(3)** All units will review their OPSEC critical information and EEFI, and ensure their EEFI is promulgated within their command. Commanders at all levels will develop OPSEC measures to ensure their classified and unclassified but sensitive information is protected in accordance with CJCSI 3213.01, reference (v).

**(4)** Physical security assessment checklists are contained in Annex M, Appendix 2 to assist commanders in conducting installation/activity AT/FP Vulnerability Assessments and Program Reviews, as well as providing common standards for all assessment teams.

**(5)** As Vulnerability Assessments are conducted throughout the AOR, patterns emerge. To give visibility to these trends and potential solutions, summarized data has been placed in the USEUCOM Vulnerability Assessment Management Program (VAMP) database. See Annex M, Appendix 2.

**(6) Antiterrorism/Force Protection Planning.** Each USEUCOM installation or site shall have in place a published and signed an AT/FP plan. These plans may be in the form of an OPLAN, OPORD or other comparable document, but in all cases they must be comprehensive, provide implementing instructions for the policies, procedures and requirements in this OPORD, and proven to be executable. DoD elements under the security authority of the COM may use guidance in this OPORD to assist in the development of AT/FP operating instructions, but should follow the guidance provided by the COM and design their plans as supporting documents to the U.S. embassy Emergency Action Plan (EAP). Standardized AT/FP plans should be tailored to specific missions and locations.

## FOR OFFICIAL USE ONLY

(a) AT/FP plan content and requirements shall include, as a minimum, the following information and program elements:

<input type="checkbox"/> (1) Terrorism Threat Assessment (classified as appropriate, and may be published under separate cover).
<input type="checkbox"/> (2) Vulnerability Assessment process to determine susceptibility to attack by the broad range of terrorist threats to the security of facilities, personnel and missions.
<input type="checkbox"/> (3) Risk Assessment process to integrate the Threat and Vulnerability Assessments to examine possible terrorist event likelihood and consequences. The Risk Assessment process will be used as a means of making conscious and informed decisions to commit resources to reduce vulnerabilities, enact policies and procedures to mitigate the threat, and to determine an acceptable the level of risk.
<input type="checkbox"/> (4) Locally tailored actions to be taken during each Force Protection Condition and Terrorist Incident Response Measures to be taken in the event terrorist action. When included in an AT/FP Plan, the complete listing of site-specific AT/FP measures, linked to a Force Protection Condition, will be classified, as a minimum, CONFIDENTIAL.
<input type="checkbox"/> (5) Procedures for reporting terrorist events or suspicious activity.
<input type="checkbox"/> (6) Alert notification procedures used to disseminate information, warnings or instructions.
<input type="checkbox"/> (7) Map(s) showing the locations of Mission Essential or Vulnerable Areas (MEVA), and when applicable, residential locations.
<input type="checkbox"/> (8) List and location of office emergency equipment (if applicable).
<input type="checkbox"/> (9) Total number of units and personnel assigned. When warranted by the threat or local circumstances, include identities of all personnel and family members (if present).
<input type="checkbox"/> (10) Consequence Management Measures. These may be part of the AT/FP plan or published in a separate document. This element covers the full range of emergency response and disaster planning actions to mitigate and recover from the effects of a terrorist attack. It should be comprehensive to include actions to take for those personnel who reside or work at off-installation sites.
<input type="checkbox"/> (11) Procedures for the review and exercise of all facets of AT/FP plans/operating instructions annually. Results should be used to facilitate program enhancements and validate that the AT/FP plan is executable.
<input type="checkbox"/> (12) Establishment of an AT/FP Working Group (or other comparable forum) to assist in program coordination, plan development, exercises, and execution. This forum should be used to track and fix identified deficiencies.

(b) Installation/activity AT/FP plans must incorporate tenant activities that reside on an installation or for whom the host provides AT/FP coverage, e.g., Area Support Group plans include all activities identified as being within their area of responsibility. Tenant activities, depending on their organization and mission, should contribute in an appropriate manner to the execution of the AT/FP plan and/or program, based upon the mutual agreement of the tenant and the host. If there is disagreement between host and tenant over the level and nature of participation by a tenant in the

## FOR OFFICIAL USE ONLY

AT/FP plan or program, the issue should be raised through the chain of command for resolution.

(7) Reporting procedures and dissemination of terrorist threat and AT/FP information are contained in Annex B, Appendix 3, and Annex C, Appendix 2.

(8) All USEUCOM Service component commands and other supporting units/activities will implement training programs that incorporate an annual AT/FP exercise for all assigned personnel. The scope, type, methodology, length, and execution of this exercise is at the discretion of the local commander with responsibility for the installation/site. However, as a minimum, the exercise should incorporate the most recent and/or likely terrorist threat scenarios.

(9) Immediate response to a crisis is critical to the recovery and continuing mission of the unit and/or headquarters affected. An installation's crisis action response must be exercised on a periodic basis, at least annually and more frequently for deployed units with a high rotational cycle or in locations designated as having High or Significant Terrorism Threat Levels.

(10) **Operational Constraints.** Commanders at all levels have to weigh mission accomplishment against the risk of terrorist incidents and endangering members of the command. However, guarding against asymmetric threats such as terrorist attacks normally enhances combat effectiveness and contributes to mission accomplishment.

### ACKNOWLEDGE:

**JOSEPH W. RALSTON**  
General, USAF

**APPENDICES:**

1. Pre-deployment Requirements
  - TAB A: Training and Equipment Requirements
2. Terrorist Force Protection Conditions
  - TAB A: Force Protection Condition Measures
  - TAB B: Non-Controlled/Off-Installation Facility Security Strategy
  - TAB C: Procedures for the Use of Deadly Force
3. Weapons of Mass Destruction (WMD)
4. United States Defense Representative (USDR) Security Responsibilities and Procedures
5. AT/FP Forums
  - TAB A: General/Flag Officer Antiterrorism Steering Group
  - TAB B: USEUCOM Joint Antiterrorism Working Group
6. Crisis Action Response
7. Readiness reporting and the Theater Security Planning System

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**C-12**  
**FOR OFFICIAL USE ONLY**



**FOR OFFICIAL USE ONLY****APPENDIX 1 (PRE-DEPLOYMENT REQUIREMENTS) TO ANNEX C (OPERATIONS)  
TO USCINCEUR AT/FP OPOD 01-01****REFERENCES: See Basic Order**

**1. SITUATION.** Due to the changing nature of the terrorist threat in USEUCOM AOR, Antiterrorism/Force Protection (AT/FP) planning, training, and equipment requirements are critical to mission success. Deploying units must consider AT/FP an integral part of the mission, not an afterthought. The requirements for exercises and operations are very similar, except exercises usually have the luxury of a longer planning process. Operations require the same type of planning, but with the planning cycle condensed into days or possibly hours. Each operation or exercise has different requirements and challenges.

**2. MISSION.** To provide definitive guidance regarding AT/FP considerations for commands and units deploying forces within the USEUCOM AOR.

**3. EXECUTION**

**a. Scheme of support.** This Appendix provides guidance and establishes AT/FP planning responsibilities for forces deploying to conduct operations, exercises or training in the USEUCOM AOR. The guidance is general in nature and designed so that units can adapt it to a particular deployment. Tab A to this Appendix lists minimum training and equipment requirements for any deployment within the USEUCOM AOR.

**b. Tasks to subordinate units**

**(1)** Commanders of the Service components, Task Forces, Joint Task Forces, Combined Task Forces, and deploying units (down to battalion, squadron, and ship level) controlling, participating in, or supporting an operation or exercise are responsible for ensuring an Antiterrorism Officer (ATO) is appointed to serve as the subject matter expert on AT/FP matters for the command. Smaller units (e.g., company, flight) must also meet this requirement when deploying without their higher headquarters, unless deploying as a subordinate element to a unit that will have an ATO.

**(2)** Ensure the ATO is trained to employ methods to reduce risk or mitigate the effects of a terrorist attack. The ATO must also be familiar with pre-deployment AT/FP training requirements. Assignment as the ATO may be a collateral or additional duty for the individual appointed.

**(3)** Ensure the ATO has attended an approved Level II AT/FP course of instruction prior to the deployment. NOTE: Commanders (in the grade of O6 or above) may waive this requirement for a period no to exceed six months if they appoint an individual who has had formal AT/FP training and/or experience in unit/individual protection programs, e.g., military police, security forces, special agents. Commanders

**FOR OFFICIAL USE ONLY**

may continue to waive formal level II training for personnel who only provide Level I training, given they have sufficient background and experience.

(4) Consider deploying the ATO early in the flow of deploying forces to execute AT/FP tasks which are requisite to the deployment, e.g., site survey/ assessment, coordination of security requirements with host nation. Typically, USEUCOM deploys a EUCOM Survey and Assessment Team (ESAT) to conduct an initial on-scene assessment of the area of operations. The ESAT will assess and report AT/FP requirements for the operation.

(5) Ensure proper AT/FP planning occurs and is executed properly. Specific planning factors vary with each operation, but the following represent basic issues to consider:

(a) Based on the nature of the operational mission, develop a prioritized list of AT/FP factors for site selection/survey teams. Use these criteria to determine if facilities, either currently occupied or under consideration for occupancy by DoD personnel, can adequately protect occupants against terrorist attack.

(b) Do not assume existing or host units at the site automatically will provide AT/FP. Likewise, do not assume the host nation will provide adequate security. All deployed DoD elements should have some type of inherent security capability, based on the mission, as well as 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. Close coordination between the deploying force and HQ USEUCOM is required to ensure all AT/FP requirements are rapidly determined.

(c) AT/FP requirements must be factored into Time Phased Force Deployment Data (TPFDD) planning. Lift requirements and timing the arrival of AT/FP assets may impact adversely on mission capability if not carefully planned.

**c. Coordinating instructions.**

(1) Host nation restrictions and sensitivities may limit AT/FP options; therefore, early coordination with the USDR should be affected to resolve issues.

(2) By their nature, contingency operations are time constrained, and each operation has unique challenges. AT/FP should be factored into the planning process from the beginning. AT/FP guidance must appear in all Warning, Planning, Alert, Deployment, or Execute Orders.

(3) Regardless of the nature of an operation or exercise, it is incumbent upon the parent command to ensure that all deploying personnel are properly trained and

**FOR OFFICIAL USE ONLY**

equipped, not only for the mission at hand, but also for force protection and personal security.

**(4)** All deploying units must comply with the provisions of Annex C, Appendix 1, Tab A, Training and Equipment Requirements. Process requests for deviations (exceptions, waivers, and variances) through the chain of command as outlined in Annex M, Appendix 1.

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
**General, USAF**

**TABS:**

A. Training and Equipment Requirements

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

## FOR OFFICIAL USE ONLY

### TAB A (TRAINING, SCREENING, AND EQUIPMENT REQUIREMENTS) TO APPENDIX 1 (PREDEPLOYMENT REQUIREMENTS) TO ANNEX C (OPERATIONS) TO USCINCEUR AT/FP OPO RD 01-01

#### 1. CATEGORIES OF TRAVELERS TO THE USEUCOM AOR.

**a. Category “A” Travelers.** Deployment/Mobilization/TDY/TAD and family member travelers, NOT traveling to support training mission exercises, deployments, and permanent change of station (PCS). These normally include TDY/TAD visitors traveling for short duration to attend scheduled conferences, meetings, and other routine functions. AT/FP training requirements for Category “A” travelers are contained in paragraph 2a, below.

**b. Category “B” Travelers.** Deployment/Mobilization/TDY/TAD travelers, traveling to support training missions, exercises, deployments, and permanent change of station (PCS). The requirements in paragraphs 2-4, below, apply. Requirements in paragraph 2, below (and in certain cases, requirements in paragraph 3-4), may apply to family members traveling PCS. The gaining command will determine modifications, as appropriate, to these requirements. In most cases, the gaining command will provide individual augmenters and PCSing personnel required equipment.

**2. TRAINING REQUIREMENTS.** Sourcing agencies (USCINCFJCOM, Services, supporting CINC’s, Defense Agencies, etc.) will ensure the following requirements are met prior to the deployment of forces to the USEUCOM AOR:

**a. Training.** All personnel traveling to the USEUCOM AOR must receive required training (classroom instruction or required reading) from their parent unit/command prior to initiating travel. This training must be provided by qualified personnel. Once this annual requirement is satisfied, additional training prior to TDY/TAD to another country may be limited to country specific AT/FP awareness. See Annex M, Appendix 1 for more detailed guidance and criteria. As a minimum, required instruction will encompass the following topics:

<input type="checkbox"/> Introduction to Terrorism*
<input type="checkbox"/> Terrorist Operations*
<input type="checkbox"/> Detecting Terrorist Surveillance*
<input type="checkbox"/> Individual Protective Measures*(issue JS Guide 5260 or equivalent publication).*
<input type="checkbox"/> Hostage/Kidnap Situation Training.*
<input type="checkbox"/> A briefing on the current country-specific Force Protection Conditions in effect.*
<input type="checkbox"/> Instruction on recognizing and reporting improvised explosive devices (IED); e.g., in packages, baggage, motor vehicles.*
<input type="checkbox"/> Country specific antiterrorism awareness brief(s), based on area(s) to be visited.*
<input type="checkbox"/> Mine Awareness Training, as applicable.
<input type="checkbox"/> Medical threat briefing and medical self-aid/buddy care.

C-1-A-1

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

- |  |
|--|
| <input type="checkbox"/> Cultural aspects of host country(ies).  |
| <input type="checkbox"/> Rules of Engagement, as applicable.   |
| <input type="checkbox"/> Command's standard OPSEC measures and EEFI.   |
| <input type="checkbox"/> Use of Deadly Force, as applicable. All forces deploying to support USEUCOM operations will ensure their personnel receive mandatory "Use of Deadly Force/ROE" training, as applicable. The training will be location specific with threat-based scenarios to compliment the training and orientation process. Coordinate training plans with all servicing Staff Judge Advocate General offices, as well as the senior Military Police/Security Forces' official on station. |

Astrik (\*) indicates required Level I AT/FP training (see Annex M, Appendix 5).

**b.** All personnel must be proficient in individual NBC defense survival skills as prescribed by Service directives. Units must be proficient in the employment of unit-level NBC equipment.

**c.** Deploying personnel must be qualified in accordance with Service regulations on assigned weapon(s). Authority to deploy with weapons/ammunition will be indicated in the exercise planning directive, unit deployment order, or augmentation tasker message.

### 3. MEDICAL

**a. Responsibilities.** Commanders are responsible to ensure health threat briefings, pre-deployment briefings and pre-deployment health screenings are conducted. All personnel deploying must be assessed and determined to be medically and psychologically fit for worldwide deployment. Based on the mission, vulnerability assessment teams may include medical personnel with preventive medicine background to evaluate commands, personnel and facilities.

**b. Medical Force Protection Requirements.** All personnel must meet the requirements as published in USEUCOM Directive 67-9 and USEUCOM preventive medicine guidance provided at <http://www.eucom.mil/hq/ecmd/prevmed/index.htm> on the NIPRNet. Health promotion, medical surveillance, and the prevention of illness, non-battle injury and disease, to include combat stress, will be integrated in the training of individual Service members, in the training of military units, and in military exercises.

**4. EQUIPMENT REQUIREMENTS.** Parent units will issue all required organizational equipment prior to deployment. USEUCOM provides clothing and equipment support to HQ USEUCOM assigned personnel only.

#### **a. Uniform**

## FOR OFFICIAL USE ONLY

(1) Personnel arriving in the AOR via commercial means will wear civilian clothing. Military personnel traveling via military/military contract transportation will wear the uniform prescribed in the applicable deployment orders.

(2) The prescribed uniform for the USEUCOM AOR is each Service's utility uniform (e.g., Army and Air Force: camouflage BDU; and Marines: utilities) depending on functional responsibilities, (e.g., aviation personnel wear flight uniforms depending on duty status).

(3) Individuals should deploy with their Service-dependent field uniform (e.g. helmet, web belt, suspenders, canteens, flak vest, etc.).

(4) Deploying personnel must bring sufficient uniform items to accomplish their mission. These items may include boots, hats, belts, field jackets, hot and/or cold weather gear, etc.

**b. Protective Equipment.** As the mission and threat indicators dictate, units deploying to the USEUCOM AOR will have their personnel deploy with the following protective equipment (may be maintained by parent unit). Parent headquarters may consider stockpiling protective equipment at deployment location for missions with high personnel turnover/frequent unit rotations. HQ USEUCOM or the gaining Service component command will notify the supporting command via OPORD, EXORD, or other message if this requirement is valid and what modifications to the below list are necessary.

<input type="checkbox"/> Protective mask with filter
<input type="checkbox"/> Filters for mask (4 each)
<input type="checkbox"/> Protective Overgarment (MOPP suit) (2 each)
<input type="checkbox"/> Protective Gloves with inserts (4 each)
<input type="checkbox"/> Protective Overboots (2 each)
<input type="checkbox"/> Hood (4 each)
<input type="checkbox"/> M-8 paper pack (2 each)
<input type="checkbox"/> Individual decontamination kits (2 each)
<input type="checkbox"/> Permethrin pretreated uniforms (2 each)
<input type="checkbox"/> Permethrin pretreated bed net and poles
<input type="checkbox"/> Extended duration DEET lotion insect repellent (2 tubes)
<input type="checkbox"/> Occupational protective equipment as required (ear plugs, gloves, respirators, etc.)

**NOTE:** Deployment orders for specific contingencies, operations and/or exercises will contain additional guidance regarding mission unique equipment and uniform requirements.

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**C-1-A-4**  
**FOR OFFICIAL USE ONLY**



**FOR OFFICIAL USE ONLY****APPENDIX 2 (TERRORIST FORCE PROTECTION CONDITIONS) TO ANNEX C (OPERATIONS) TO USCINCEUR AT/FP OPORD 01-01**

- REFERENCES:**
- a. DoD Directive 2000-12, DoD Antiterrorism/Force Protection Program, 13 Apr 99
  - b. DoD Instruction 2000-16, DoD Antiterrorism Standards, 8 Jan 01
  - c. DoD Handbook 2000.12H Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence, 19 Feb 93 with Change 2

**1. SITUATION.** An effective AT/FP program requires the efforts of the entire USEUCOM community. Because of the nature and dynamics of terrorism, commanders must constantly review their programs and defensive posture designed to thwart and deter the terrorist. These programs and postures must be constantly reviewed and updated as required. Units/activities must carefully orchestrate and coordinate AT/FP efforts to preclude duplication of effort, while putting forth a timely and appropriate response. Proper protective measures, prudently implemented, can have a significant deterrent effect on terrorist actions. Even if not completely effective in deterring a terrorist act, protective measures can serve to limit damage and save lives.

**2. MISSION.** To provide guidance and procedures for commanders at all levels to execute an effective defensive posture (Terrorist Force Protection Condition (also referred to as Force Protection Condition or FP CON, and formerly known as THREATCON) to thwart terrorist attacks, and to rapidly and smoothly transition from one Force Protection Condition to another when dictated by the threat or other conditions.

**3. EXECUTION**

**a. Scheme of support.** Nothing in this appendix shall detract from, nor be construed to conflict with, the authorities and responsibilities of the U.S. Combatant Commanders, or the inherent responsibility of designated military commanders to protect military installations, equipment, and personnel under their command.

**(1)** Commanders at the Colonel/Captain (O-6) level (e.g., Military Communities, Air Bases, or geographically separated units) normally will declare the Force Protection Condition for their units. This approach ensures the execution of the most appropriate response to an assessed threat for a specific area, installation/site, or unit/command. Higher level commanders in the chain of command may at any time exercise their prerogative to declare a Force Protection Condition for their AOR or any portion thereof.

**(2)** Service component commanders, Task Force/Joint Task Force (TF/JTF) commanders, senior U.S. members of a Combined Task Force (CTF) (or NATO/UN

**FOR OFFICIAL USE ONLY**

commands), Direct Reporting Units (DRU), and U.S. Defense Representatives (USDR), or their designated representatives, may declare an appropriate Force Protection Condition for their forces within geographical areas based on the assessed terrorist threat for that area.

(3) When a terrorist threat against DoD interests in a particular area of USEUCOM affects more than one Service component commander, the USEUCOM Deputy Commander-in-Chief (DCINCEUR) is responsible to ensure a uniform military response to the threat.

(4) Force Protection Conditions normally are based on terrorist threat assessments produced by assigned or supporting terrorism intelligence analysts combined with a determination of host-nation authorities and component/base/unit capabilities to implement and sustain security measures, and the overall impact of the AT/FP measures upon the organization's mission. However, the Terrorism Threat Level does not dictate the specific Force Protection Condition to assume. Commanders are responsible for Force Protection Condition declarations and should consider the value of particular areas, installations/sites and facilities as targets, along with any special vulnerabilities.

(5) Each Force Protection Condition is designed to produce a detection, assessment, and response capability commensurate with the existing terrorist threat. Escalating the Force Protection Condition should enhance these capabilities and send a clear signal of increased readiness.

(6) Tab A to this Appendix describes security measures associated with each Force Protection Condition. These measures are the minimum for each Force Protection Condition. Commanders may direct more intensive security precautions when implementing a given Force Protection Condition. When local conditions warrant, subordinate commanders may request a reduction of the Force Protection Condition prescribed by higher authority, or reduce certain required security measures in accordance with paragraph 1e, Tab A to this Appendix.

(7) Subordinate commands will notify HQ USEUCOM of increased or decreased Force Protection Conditions as rapidly as practical, usually through OPREP channels. Voice reporting should be followed by a message providing the following information, as a minimum:

(a) Brief description of circumstances that resulted in Force Protection Condition change.

(b) The Force Protection Condition change, its effective date/time, anticipated duration of new posture and, if applicable, additional instructions, e.g., "Force Protection Condition CHARLIE implemented from 251200Z Dec 98 to 021200Z

**FOR OFFICIAL USE ONLY**

Jan 99"; or "Effective upon receipt and until further notice, Force Protection Condition BRAVO plus Measures 37, 38, and 43 implemented."

(c) Specific location/unit(s), geographical region, or country affected by the Force Protection Condition change.

(8) HQ USEUCOM, through the Joint Analysis Center's Directorate of Operations, Analysis Division, Terrorism/Counterintelligence Analysis Branch (JAC-DOAT), publishes monthly summaries of the assessed terrorist threat for each country in the theater. These summaries are available at: <http://www.jac.eucom.smil.mil/>. ECSCM provides updates on Force Protection Condition status throughout the theater; these daily updates are provided to the European Theater Command Center (ETCC) and are available at: <http://www.eucom.smil.mil/ecj3/etcc/main.html>.

(9) When implementing any Force Protection Condition, commanders should give particular attention to policies and procedures governing the issuance and use of firearms. During implementation of security measures associated with Force Protection Condition CHARLIE and, as appropriate, other Force Protection Conditions, local orders must include instructions on issuing weapons/live ammunition and the use of deadly force.

(10) To introduce an element of unpredictability into the system, various security measures from higher Force Protection Conditions should be randomly implemented based on a commander approved plan. The application of Random Antiterrorism Measures (RAM) will increase AT/FP alertness and awareness as well as providing opportunities to train on implementing higher level Force Protection Condition security measures. A RAM program may also make it harder for terrorists to predict movement or activity at a given location. Assume terrorists are conducting surveillance. Place emphasis on detecting such activity at every stage of security alert.

(11) Normally, the Force Protection Condition at any given location will be unclassified; however, compilations showing a complete listing of site-specific AT/FP measures associated with the Force Protection Condition will be classified, as a minimum, CONFIDENTIAL, when included in the installation AT/FP Plan. When separated from the AT/FP plan, individual or a less than complete listing of site-specific AT/FP measures associated with the Force Protection Condition remain FOR OFFICIAL USE ONLY. The security readiness posture throughout the theater or an entire country, or orders directing Force Protection Condition changes, may be classified when appropriate. Particular attention should be given to safeguarding intelligence information related to Force Protection Condition changes while at the same time providing unclassified "tear lines" for use in briefing local communities and security forces.

**b. Tasks and Responsibilities****C-2-3****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****(1) DCINCEUR**

(a) Exercise the authority of the USCINCEUR pursuant to DoDD 2000.12, reference (a), to ensure the Force Protection Condition system is implemented uniformly throughout USEUCOM for the protection of DoD personnel, their family members, facilities, and resources.

(b) Assess the Terrorism Threat Levels within the theater and publish monthly summaries of the assessed terrorist threat throughout the theater.

(c) Inform SHAPE, the Joint Staff, other CINCs, HQ USEUCOM staff, subordinate commanders, any DRUs, and COMs, of the nature and degree of local threats. Ensure commanders are prepared to respond to threat changes.

(d) Declare appropriate Force Protection Conditions based upon guidelines in this Appendix.

(e) When down-channeling a command directed Force Protection Condition change, make the following notifications in addition to component commands and DRUs: SHAPE (U.S. Survey Section), the National Military Command Center (NMCC), and all COMs who may be impacted by the threat or circumstances causing the change. When HQ USEUCOM receives an up-channeled Force Protection Condition change, notify the same organizations/activities listed above.

**(2) Service component commanders, TF/JTF commanders, senior U.S. members of a CTF (or NATO/UN commands), DRU's, and USDR's.**

(a) Prepare terrorism threat assessments for their AOR using the guidelines in DoDD 2000.16, reference (b). These assessments along with the guidance in paragraph 3a, above, will be used to determine an appropriate Force Protection Condition baseline.

(b) Publish guidance outlining procedures for implementing the Force Protection Condition system, which as a minimum will require subordinate commands to:

(1) Annually test the Force Protection Condition up-channel, down-channel and lateral notification system. Actual implementation will satisfy this requirement.

(2) Advise the chain of command of any Force Protection Condition changes by initiating up-channel, down-channel and lateral notification to all DoD elements and personnel who may be impacted by the change/threat. Give particular attention to notifying all elements and personnel deployed TDY/TAD to the command's location.

(3) Develop preplanned AT/FP measures tailored to local circumstances for each Force Protection Condition. Installation/site commanders will

**FOR OFFICIAL USE ONLY**

coordinate Force Protection Condition implementation with host nation military and police authorities when appropriate.

(4) Identify local critical and/or mission essential areas and activities, high risk individuals, and off-installation areas frequented by DoD personnel. Develop pre-planned protective measures for these potential terrorist targets and include these measures within each Force Protection Condition as appropriate.

(5) Implement higher headquarters-directed Force Protection Condition changes immediately upon receipt of notification.

(6) To assist in maximizing coordination of security responses to terrorist threats, include the following as information addressees when disseminating Force Protection Condition changes:

HQ USEUCOM VAIHINGEN//ETCC/ECSSM//  
 USCINCEUR ALT SHAPE BE//SPASAC//  
 CDRUSAREUR HEIDELBERG GE//AEAGC/AEAGC-O-FP//  
 USAREUR PROVOST MARSHAL MANNHEIM GE//PM//  
 CINCUSNAVEUR LONDON UK//N3/N34//  
 HQ USAFE RAMSTEIN AB GE//SF/IN/IV//  
 USAFE AOS RAMSTEIN AB GE//CAT-DIR/AOC//  
 COMMARFOREUR BOBLINGEN GE//FP/G2/G3//  
 COMSOCEUR VAIHINGEN GE//CS/J2/J3//  
 AIG 4530

(7) Immediately report any incident, threat, surveillance, or suspicious activity that may have an impact on the AT/FP posture within the USEUCOM AOR. Use guidance in CJCSM 3105.03, reference (u) in Basic Order, to notify the chain of command of any activity that may impact AOR AT/FP posture. Additionally,

(a) Use any form of communication available when the information is time critical, including E-mail and the various military communication/computer nets.

(b) Pass terrorist threat and other related intelligence information as quickly as possible to all affected DoD elements, commands and the USDR. Disseminate relevant information to the lowest level in the most efficient manner available.

(8) In all cases, coordinate release of threat information of a general nature with the USDR. The COM places particular attention to this coordination and the scope/nature of the threat to ensure compliance with the USG "No Double Standard" policy. As defined in DoDD 2000.12, reference (a), the "No Double Standard" policy means that terrorist threat alerts, threat advisories, and/or Terrorist Threat Warning Reports (TWRs) must be disseminated to all American citizens, if the general public is included in, or can be construed as part of, the terrorist targeting. DOS is the sole approving authority for releasing terrorist threat information to the public, and the COM normally affects the coordination required prior to releasing the information.

**(3) HQ USEUCOM Staff**

C-2-5

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

(a) Establish internal procedures to notify assigned staff members who are deployed TDY/TAD when threat warnings are issued, terrorist incidents occur, and/or Force Protection Condition changes/increases are declared that may impact on their mission. This includes HQ USEUCOM staff members deployed or TDY/TAD in support of training, exercises, operations or on trips to conferences, meetings, assessments, and/or other routine functions.

(b) Whenever USCINCEUR or DCINCEUR directs specific AT/FP measures or establishes a baseline Force Protection Condition of BRAVO or higher, be it theater-wide, in a specific region, country and/or location, track the notification of all HQ USEUCOM deployed or TDY/TAD staff members using the following guidelines:

(1) Upon receipt of a message increasing the Force Protection Condition, each staff directorate and special staff office will provide input to the ETCC using the matrix in Table C-2-1, below, as a tool to verify/track that all staff members have received the information. The ETCC will collate and maintain staff directorate and special staff reports.

(2) The sponsoring directorate or special staff office is responsible for the personnel accountability of its deployed staff members. The sponsoring directorate/special staff office will contact the element leader and/or personnel deployed to locations that may be impacted by this change to ensure the deployed elements/personnel are aware of the threat and take appropriate action in coordination with their hosts.

(3) The sponsoring directorate/special staff office also should assess the merits of continuing or discontinuing the mission or trip. Considerations should include, but not be limited to: mission criticality; AT/FP available; nature of the threat warning; terrorist incident; and/or Force Protection Condition increase; etc.

(4) Directorates and special staff offices will provide the information back to the ETCC using the format provided in Table C-2-1, below, within 12 hours of receipt of a message increasing the Force Protection Condition and provide additional updates every 12 hours as required. Even if all staff members are on station, notify the ETCC. If unable to contact deployed staff members directly, notify the ETCC who will assist in contacting the host to verify notification.

**Table C-2-1: Sample Force Protection Condition Notification Matrix**

<b>Event: USCINCEUR Force Protection Condition Increase to BRAVO in the Balkans (FRY, FYROM, B-H, Croatia, Slovenia) (notional sample)</b>						
<b>Sponsor/ Host</b>	<b>Element</b>	<b>Purpose</b>	<b>Location</b>	<b>Dates</b>	<b>Advised of Force Protection Condition Change</b>	<b>Recmnd: Recall or Remain</b>
ECJ5/ Amemb Croatia	Staff Team	Coordinate NEO Plan	Zagreb	3-9 Feb	Yes: 041800Z Feb	Remain
ECSM/ Amemb	VA Assess	Assess Camp Able	FYROM	2-5 Feb	Yes 042000Z	Remain

**C-2-6**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

Skopje	Team	Sentry			Feb	
ECMD/ KFOR	Maj Dokes	Survey	Kosovo	2-5 Feb	Yes 042130Z Feb	Recall
ECJ2/ KFOR	CDR Bond	Augmentation	Pristina, Kosovo	Indef	Yes 042132Z Feb	Remain
ECJ4/ TF Riejka	ECJ4- JMD	Assess port facility	Riejka, Croatia	3-8 Feb	Yes 042140Z Feb	Recall

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
General, USAF

**TABS:**

- A.** Force Protection Condition Measures
- B.** Non-Controlled/Off-Installation Facility Security Strategy
- C.** Procedures for the Use of Deadly Force

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)



**FOR OFFICIAL USE ONLY****TAB A (FORCE PROTECTION CONDITION MEASURES) TO APPENDIX 2  
(TERRORIST FORCE PROTECTION CONDITIONS) TO ANNEX C (OPERATIONS)  
TO USCINCEUR AT/FP OPORD 01-01**

**1. GENERAL.** All USEUCOM DoD components shall implement the Terrorist Force Protection Condition (FPCON) system (formerly known as the THREATCON system). The FPCON system provides a common framework to facilitate inter-Service coordination, supports U.S. military AT/FP activities, and enhances overall DoD implementation of U.S. Government antiterrorist policy. A commander, agency, or organization director declares an appropriate FPCON to include locally tailored Antiterrorism/Force Protection (AT/FP) measures in accordance with the guidance in Annex C, Appendix 2.

a. All appropriate sources of information should be used to determine the appropriate FPCON and additional local AT/FP measures designed to counter specific threats and tailored to local circumstances. Sources available to make this determination include higher headquarters and local intelligence assets, law enforcement information, and command liaison, as tempered by best judgment and knowledge of the local situation. Guidelines for terrorism analysts to assess the terrorist threat are contained in Annex B. Guidelines for commanders to determine appropriate FPCONs and AT/FP measures are provided below. For Information Operations Conditions (INFOCON), see Annex K.

**b.** The DoD FPCON system and associated measures outlined in paragraph 2, below, are generally not applicable to DoD elements for which the Chief of Mission (COM) has security responsibility and may have limited application to DoD elements that are tenants on installations and facilities not controlled by U.S. military commanders. Commanders exercising TACON for force protection of such tenants and/or deployed forces will ensure these DoD elements are aware of the existing FPCON and Terrorist Threat Level. Further, these DoD elements will implement local, tailored security measures to include individual and unit security precautions consistent with the existing FPCON, and coordinate with host nation authorities regarding measures that the tenant or deployed force does not have the wherewithal to execute. Commanders will advise the U.S. chain of command of any unresolved vulnerabilities that create, in his or her judgment, an unacceptable level of risk to DoD elements, personnel and/or assets.

**c.** Each set of FPCON measures is the minimum that must be implemented when a change in the threat warrants a change in FPCON or when higher authority directs an increase in FPCON. Authorities directing implementation may add measures from higher FPCONs at their discretion. Military commanders or DoD civilians exercising equivalent authority 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. Local military commanders or DoD civilians exercising equivalent authority will not implement measures that are less rigorous than those appropriate for the declared FPCON. Waivers for not complying with prescribed FPCON measures may be obtained by following the procedures in paragraph e.

**FOR OFFICIAL USE ONLY**

**d.** To enhance the overall effectiveness of a given FPCON, commanders shall develop and implement a Random Antiterrorism Measures (RAM) program as an integral part of their AT program. RAM programs should include measures from higher FPCONs, command developed measures, and/or locally developed site-specific measures. Analysis of previous successful, and unsuccessful, terrorist operations has consistently shown most terrorist actions are the culmination of months of planning and surveillance. A properly executed RAM program presents a highly visible, constantly changing security posture, which can effectively frustrate an adversary's attempts to target our assets/activities and gain an operational advantage through surveillance.

**e.** If it is determined that certain FPCON measures are inappropriate for current operations, or for proper threat mitigation, military commanders or DoD civilians exercising equivalent authority may request a waiver. The first general/flag officer exercising TACON for force protection is the approval authority for waiver of specific FPCON measures. Any senior military commander having TACON for force protection may withdraw first general/flag officer 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 Senior Executive Service) rests with the military commander directing their execution. Nothing in this waiver process is intended to diminish the authority or responsibility of military commanders, senior to the waiver authority, from exercising oversight of FPCON and RAM program execution. Approved waivers, to include mitigating measures or actions, will be forwarded through the Component Command to HQ USEUCOM/ECSM within 24 hours.

**f.** The following standards regarding the wearing of uniforms apply to all DoD personnel in the USEUCOM AOR. These standards do not apply during military missions or operations where the wearing of uniforms is consistent with the mission and mode of travel. Commanders may establish more stringent requirements as appropriate to the threat and circumstances.

**(1)** During FPCON Normal, Alpha, and Bravo, wearing of military uniforms off U.S. installations and other controlled environments is at the discretion of the chain of command exercising TACON for Force Protection.

**(2)** During FPCON Charlie, wearing of military uniforms off U.S. installations or other controlled environments is authorized only while traveling between home and work, to official functions, and for brief, essential stops at childcare facilities or service stations.

**(3)** During FPCON Delta, military uniforms will not be worn or openly displayed off U.S. installations or other controlled environments.

**2. FORCE PROTECTION CONDITIONS.** Establish FPCONs and their associated AT/FP measures as follows: The FPCON relies on multiple factors to include, but not limited to the threat, target vulnerability, criticality of assets, security resource availability, impact on operation and morale, damage control, recovery procedures, international relations, and planned U.S. Government actions that could trigger a terrorist response.

C-2-A-2

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

a. **Force Protection Condition NORMAL.** Applies when a general global threat of possible terrorist activity exists, and warrants a routine security posture.

b. **Force Protection Condition ALPHA.** Applies when there is an increased general threat of terrorist activity against personnel and facilities, the nature and extent of which are unpredictable. It may be necessary to implement certain measures from higher FPCONs resulting from intelligence received or as a deterrent. Units must be capable of maintaining the measures in FPCON ALPHA indefinitely.

<p>❑ <b>Measure 1.</b> At regular intervals remind all personnel, and family members to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of U.S. installations, units, or facilities. Watch for abandoned parcels or suitcases or unusual activity.</p>
<p>❑ <b>Measure 2.</b> The duty officer or other appointed personnel with access to building plans as well as plans for area evacuations must be available (e.g., on-call) at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on call and readily available.</p>
<p>❑ <b>Measure 3.</b> Secure buildings, rooms, and storage areas not in regular use.</p>
<p>❑ <b>Measure 4.</b> Increase security spot checks of vehicles and persons entering installations and unclassified areas under the jurisdiction of the United States.</p>
<p>❑ <b>Measure 5.</b> Limit access points for vehicles and personnel commensurate with a reasonable traffic flow.</p>
<p>❑ <b>Measure 6.</b> On a frequent and/or daily basis, implement one or more Random Antiterrorism Measures (RAM), to include, as a deterrent, measures 14, 15, 17, or 18 from FPCON BRAVO either individually or in combination with each other. Increase the frequency, quantity and duration of RAMs in FPCON Bravo and Charlie.</p>
<p>❑ <b>Measure 7.</b> Review all plans, orders, personnel details, and logistic requirements related to the introduction of a higher FPCON, to include: availability of properly trained and equipped manpower for higher FPCONs IAW installation post priority list; quantities of security equipment (barriers, lights, sandbags, etc); and Chemical/Biological/Radiological defense capabilities (e.g., gas masks, in-place shelter plans, decontamination teams). Additionally, review Vulnerability Assessment Management Program (VAMP) data and the most recent Vulnerability Assessment report.</p>
<p>❑ <b>Measure 8.</b> As appropriate, review and implement security measures for high-risk personnel, e.g., direct use of inconspicuous body armor.</p>
<p>❑ <b>Measure 9.</b> As appropriate, consult local authorities on the threat and mutual AT/FP measures.</p>
<p>❑ <b>USCINCEUR Measure 10.</b> Commanders must enforce control of entry onto critical U.S. installations, e.g., lucrative target/high profile locations (see Glossary for further definition), and randomly search vehicles entering these areas. Particular scrutiny should be given to vehicles that are capable of concealing an IED sufficient to cause</p>

**FOR OFFICIAL USE ONLY**

catastrophic damage or loss of life (e.g., cargo vans, delivery trucks, etc.).

**c. Force Protection Condition BRAVO.** Applies when an increased and more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and relations with local authorities.

- |  |
|--|
| <p>□ <b>Measure 11.</b> Continue measure 1 above and warn personnel of any other potential form of terrorist attack. Continue, or introduce, all FPCON ALPHA measures.</p>   |
| <p>□ <b>Measure 12.</b> Keep all personnel involved in implementing antiterrorist contingency plans on call, especially members of the Threat Working Group and similar command advisory bodies.</p>   |
| <p>□ <b>Measure 13.</b> Check plans for implementation of the measures in FPCON CHARLIE and consider staging equipment (e.g., barriers, portable lights, etc.).</p>  |
| <p>□ <b>Measure 14.</b> Move cars and objects (e.g., crates, trash containers, etc.) at least 25 meters from buildings, particularly buildings of a sensitive or prestigious nature (applies to critical and primary gathering structures as determined by the installation commander). Apply this criterion to all inhabited structures to the greatest extent possible where feasible. Consider centralized parking on the installation or in areas with constant patrol coverage. Any parking within 25 meters of critical structures (as determined by the installation commander) must incorporate mitigation measures (e.g., inspections of vehicles for large IEDs,** designated parking with requirement that vehicle operators inspect their vehicles, etc.).</p> <p>** At a minimum, vehicle compartments capable of concealing a duffle bag size item should be inspected since this is the approximate volume required to contain an IED with an explosive equivalent of 100kg of TNT. See Annex D, Appendix 1 for more data on blast effects.</p> |
| <p>□ <b>Measure 15.</b> Secure and regularly inspect all buildings, rooms, storage areas, access points to heating, ventilation and air conditioning systems, and back-up generator rooms when not in regular use.</p>   |
| <p>□ <b>Measure 16.</b> At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious items, e.g., vehicles/large containers in unauthorized areas, unlocked access to ventilation systems, or indicators of possible facility/personnel surveillance.</p>  |
| <p>□ <b>Measure 17.</b> Examine (above the regular examination process) mail for letter or parcel bombs. .</p>   |
| <p>□ <b>Measure 18.</b> Check all deliveries to messes, clubs, etc. Advise family members to check home deliveries. Consider limiting times for delivery vehicles to enter the installations to maximize use of explosive detector dog teams and/or vehicle search teams.</p>  |
| <p>□ <b>Measure 19.</b> As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs and other soft targets to improve</p>  |

**FOR OFFICIAL USE ONLY**

deterrence and defense, and to build confidence among staff and family members.
<input type="checkbox"/> <b>Measure 20.</b> Make staff and family members aware of the general situation in order to stop rumors and to prevent unnecessary alarm.
<input type="checkbox"/> <b>Measure 21.</b> At an early stage and within guidelines for release of sensitive and/or classified information, notify members of host nation police and security services of any action being taken and why.
<input type="checkbox"/> <b>Measure 22.</b> Physically inspect visitors and randomly inspect their suitcases, parcels, and other containers. Ensure proper dignity is maintained. If possible, ensure only females qualified to conduct physical inspections perform these inspections of female visitors. Do not limit application to installation entry points; include inhabited structures, billeting and primary gathering facilities.
<input type="checkbox"/> <b>Measure 23.</b> Operate random patrols to check vehicles, people, and buildings on all U.S. installations and housing areas.
<input type="checkbox"/> <b>Measure 24.</b> Protect off-base military personnel and military transport in accordance with prepared plans. Remind drivers to lock parked vehicles and to check before entering or exiting the vehicle.
<input type="checkbox"/> <b>Measure 25.</b> Implement additional security measures for High Risk Personnel, as appropriate.
<input type="checkbox"/> <b>Measure 26.</b> Brief personnel who may augment guard forces on the use of deadly force and/or rules of engagement. Ensure there is no misunderstanding of these instructions.
<input type="checkbox"/> <b>Measure 27.</b> As appropriate, consult local authorities on the threat and mutual AT measures.
<input type="checkbox"/> <b>Measures 28 through 29.</b> Additional measures to be determined by subordinate commands, usually at installation/site level.

**Note:** If security augmenters are posted during either FPCON ALPHA or BRAVO (implementing individual measures from FPCON CHARLIE or DELTA), these augmenters must either be armed (issued a weapon with ammunition) or have armed over-watch. Ensure personnel who are armed have received required training per Measure 26 (FPCON BRAVO).

**d. Force Protection Condition CHARLIE.** Applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel or facilities is likely. Implementation of CHARLIE measures will create hardship and affect the activities of the unit and its personnel. To sustain this posture for an extended period, augmentation normally will be required.

<input type="checkbox"/> <b>Measure 30.</b> Continue, or introduce, all Force Protection Condition BRAVO measures.
<input type="checkbox"/> <b>Measure 31.</b> Keep either the primary or alternate personnel, who are responsible for implementing antiterrorist plans at their places of duty (e.g., installation/activity).
<input type="checkbox"/> <b>Measure 32.</b> Limit access points to the installation/activity and each facility to the absolute minimum.

**FOR OFFICIAL USE ONLY**

- **Measure 33.** Enforce control of entry onto all U.S. installations, housing areas, and into U.S. facilities not located on U.S. controlled installations and randomly search vehicles entering these areas.

At U.S. controlled installations, search all large vehicles capable of concealing an IED sufficient to cause catastrophic damage or loss of life (e.g., cargo vans, delivery trucks, etc.). Establish local procedures to accommodate situations where such delivery vehicles are locked/sealed. These vehicles need not be searched if associated documents and inspections by competent, trusted authority can be verified.

- **Measure 34.** Enforce centralized parking of vehicles away from sensitive buildings.
- **Measure 35.** Issue weapons to guards. Local orders should include specific instructions on issuing live ammunition. (see note).
- **Measure 36.** Increase patrolling of the installation.
- **Measure 37.** Protect all designated mission essential/vulnerable areas (MEVA). Give special attention to MEVAs and facilities not located on controlled installations.
- **Measure 38.** Erect barriers and obstacles to control traffic flow, provide stand-off and/or establish enclaves within the installations/activities.
- **Measure 39.** Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to terrorist attacks.
- **Measure 40.** Additional measures to be determined by subordinate commands, usually at installation/site level.

**e. Force Protection Condition DELTA.** Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods.

- **Measure 41.** Continue or introduce all measures listed for FPCONs BRAVO and CHARLIE.
- **Measure 42.** Augment guards, as necessary.
- **Measure 43.** Identify all vehicles already on the installation within operations or mission support areas.
- **Measure 44.** Search all vehicles and their contents before allowing entrance to the complex or installation.
- **Measure 45.** Control access and implement positive identification of all personnel -- no exceptions.
- **Measure 46.** Search all suitcases, briefcases, packages, etc., brought into the complex or installation.
- **Measure 47.** Strictly control access to all areas under the jurisdiction of the United States.
- **Measure 48.** Make frequent checks of the exterior of buildings and parking areas for suspicious items, e.g., vehicles/large containers in unauthorized areas, unlocked



**FOR OFFICIAL USE ONLY**

access to ventilation systems, or indicators of possible facility/ personnel surveillance.
<input type="checkbox"/> <b>Measure 49.</b> Minimize all administrative journeys and visits.
<input type="checkbox"/> <b>Measure 50.</b> Coordinate the possible closing of public and military roads and facilities with local authorities.
<input type="checkbox"/> <b>Measure 51.</b> Consider terminating all non-mission essential activities (e.g., AAFES, DECA, MWR).
<input type="checkbox"/> <b>Measure 52 and beyond.</b> Additional measures to be determined by subordinate commands, usually at installation/site level.

**3. COMBATANT SHIPBOARD FORCE PROTECTION CONDITIONS.** The measures outlined below are for use aboard vessels and serve two purposes. First, the crew is alerted, additional watches are created, and there is greater security. Second, these measures display the ship's resolve to prepare for and counter the terrorist threat. These actions are designed to convey to anyone observing the ship's activities that the ship is prepared, the ship is an undesirable target, and the terrorist(s) should look elsewhere for a vulnerable target. The measures outlined below do not account for local conditions and regulations, special evolutions, or current threat intelligence. The ship's command must maintain flexibility. As threat conditions change, the ship's crew must be prepared to take actions to counter the threat. When necessary, additional measures must be taken immediately. While the simple solution to Force Protection Condition CHARLIE or DELTA is to get underway, this option may not always be available.

**a. Force Protection Condition ALPHA.** Declare Force Protection Condition ALPHA when a general threat of possible terrorist activity is directed toward installations and personnel, the nature and extent of which are unpredictable, and where circumstances do not justify full implementation of Force Protection Condition BRAVO measures. However, it may be necessary to implement certain selected measures from Force Protection Condition BRAVO as a result of intelligence received or as a deterrent. Ships must be capable of maintaining Force Protection Condition ALPHA indefinitely.

<input type="checkbox"/> <b>Measure 1.</b> Brief crew on the port specific threat, the security/force protection plan, and security precautions to be taken while ashore. Ensure all hands are knowledgeable of various Force Protection Condition requirements and that they understand their role in implementation of measures.
<input type="checkbox"/> <b>Measure 2.</b> Muster and brief security personnel on the threat and rules of engagement.
<input type="checkbox"/> <b>Measure 3.</b> Review security plans and keep them available. Retain key personnel who may be needed to implement security measures on call.
<input type="checkbox"/> <b>Measure 4.</b> Secure and periodically inspect spaces not in use.
<input type="checkbox"/> <b>Measure 5.</b> Remind all personnel to be suspicious and inquisitive of strangers, be alert for abandoned parcels or suitcases and for unattended vehicles in the vicinity. Report unusual activities to the OOD.

**FOR OFFICIAL USE ONLY**

<input type="checkbox"/> <b>Measure 6.</b> Review pier and shipboard access control procedures.
<input type="checkbox"/> <b>Measure 7.</b> Ensure sentries, roving patrols and the quarterdeck watch have the ability to communicate.
<input type="checkbox"/> <b>Measure 8.</b> Coordinate pier/fleet landing security requirements with SOPA, collocated forces, and/or local authorities. Identify anticipated needs for mutual support and define methods of activation and communication.
<input type="checkbox"/> <b>Measure 9.</b> Deploy barriers to keep vehicles away from the ship if possible (400 feet minimum stand-off distance).
<input type="checkbox"/> <b>Measure 10.</b> Randomly inspect vehicles entering pier.
<input type="checkbox"/> <b>Measure 11.</b> Randomly inspect hand carried items and packages before they are brought aboard.
<input type="checkbox"/> <b>Measure 12.</b> Regulate shipboard lighting to best meet the threat environment.
<input type="checkbox"/> <b>Measure 13.</b> Rig hawsepipe covers and rat guards on lines, cables and hoses. Consider using an anchor collar.
<input type="checkbox"/> <b>Measure 14.</b> Raise accommodation ladders, stern gates, ladders, etc. when not in use.
<input type="checkbox"/> <b>Measure 15.</b> Increase frequency of security drills.
<input type="checkbox"/> <b>Measure 16.</b> Review individual actions in Force Protection Condition BRAVO for possible implementation.

**b. Force Protection Condition BRAVO.** Declare Force Protection Condition BRAVO when an increased and more predictable threat of terrorist activity exists. The measures in this Force Protection Condition must be capable of being maintained for weeks without causing undue hardships, affecting operational capability or aggravating relations with local authorities.

<input type="checkbox"/> <b>Measure 17.</b> Maintain appropriate Force Protection Condition ALPHA measures.
<input type="checkbox"/> <b>Measure 18.</b> Set material condition YOKE, main deck and below.
<input type="checkbox"/> <b>Measure 19.</b> Consistent with local rules, regulations, and/or the Status of Forces Agreement, post pier sentries as necessary.
<input type="checkbox"/> <b>Measure 20.</b> Restrict vehicle access to the pier. Discontinue parking on the pier. Consistent with local rules, regulations, and/or the Status of Forces Agreement, establish unloading zone(s) and move all containers as far away from the ship as possible (400 feet minimum stand-off distance).
<input type="checkbox"/> <b>Measure 21.</b> Consistent with local rules, regulations, and/or the Status of Forces Agreement, post additional watches. Local threat, environment and fields of fire should be considered when selecting weapons.
<input type="checkbox"/> <b>Measure 22.</b> Post signs in local language that clearly define visiting and loitering restrictions.
<input type="checkbox"/> <b>Measure 23.</b> Identify and inspect workboats, ferries and commercially rented liberty craft at least daily on a random basis.
<input type="checkbox"/> <b>Measure 24.</b> Direct liberty boats to make a security tour around the ship upon departing from and arriving at the ship with particular focus on the waterline, and under pilings when berthed at a pier.



**FOR OFFICIAL USE ONLY**

<p>❑ <b>Measure 25.</b> Inspect all hand carried items, and packages before allowing them aboard. Where available, use baggage scanners and walk through or hand held metal detectors to screen packages and personnel prior to boarding the ship.</p>
<p>❑ <b>Measure 26.</b> Implement measures to keep unauthorized craft away from the ship. Authorized craft should be carefully controlled. Coordinate with host nation/local port authority as necessary, and request their assistance in controlling unauthorized craft.</p>
<p>❑ <b>Measure 27.</b> Raise accommodation ladders, stern gates, ladders, etc. when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.</p>
<p>❑ <b>Measure 28.</b> Review liberty policy in light of the threat and revise it, as necessary, to maintain safety and security of ship and crew.</p>
<p>❑ <b>Measure 29.</b> Conduct divisional quarters at foul weather parade.</p>
<p>❑ <b>Measure 30.</b> Ensure an up-to-date list of bilingual personnel for area of operations. Maintain warning tape in pilot house/ quarterdeck, for use on the ship's announcing system that warns small craft to remain clear in both the local language and English.</p>
<p>❑ <b>Measure 31.</b> If not already armed, arm the quarterdeck watch.</p>
<p>❑ <b>Measure 32.</b> If not already armed, arm the sounding and security patrol.</p>
<p>❑ <b>Measure 33.</b> Review procedures for expedient issue of firearms and ammunition to the Shipboard Self-Defense Force (SSDF) and other members of the crew, as deemed necessary by the CO.</p>
<p>❑ <b>Measure 34.</b> Test internal and external communications. Include connectivity checks with local agencies/authorities that will be expected to provide support, if required.</p>
<p>❑ <b>Measure 35.</b> Instruct watches to conduct frequent, random searches of pier to include pilings and access points.</p>
<p>❑ <b>Measure 36.</b> Conduct visual inspections of the ship's hull and ship's boats at intermittent intervals and immediately before it puts to sea.</p>
<p>❑ <b>Measure 37.</b> Hoist ships boats aboard when not in use.</p>
<p>❑ <b>Measure 38.</b> Terminate all public visits.</p>
<p>❑ <b>Measure 39.</b> After working hours, reduce entry points to ships interior by securing infrequently used entrances. Safety requirements must be considered.</p>
<p>❑ <b>Measure 40.</b> Remove one brow if two are rigged.</p>
<p>❑ <b>Measure 41.</b> Maintain capability to get underway on short notice or as specified by SOPA.</p>
<p>❑ <b>Measure 42.</b> Consider layout of fire hoses. Brief designated personnel on procedures for repelling boarders, small boats, and ultra-light aircraft.</p>
<p>❑ <b>Measure 43.</b> Where applicable, obstruct possible helicopter landing areas.</p>
<p>❑ <b>Measure 44.</b> Where possible, monitor local communications (ship to ship, TV, radio, police scanners, etc.).</p>
<p>❑ <b>Measure 45.</b> Inform local authorities of actions being taken as Force Protection Condition increases.</p>
<p>❑ <b>Measure 46.</b> Review individual actions in Force Protection Condition CHARLIE for possible implementation.</p>

**FOR OFFICIAL USE ONLY**

**c. Force Protection Condition CHARLIE.** Declare Force Protection Condition CHARLIE when an incident occurs or intelligence is received indicating that some form of terrorist action against installations and personnel is imminent. Implementation for more than a short period will probably create hardship, affecting the peacetime activities of the ship and its personnel.

<input type="checkbox"/> <b>Measure 47.</b> Maintain appropriate Force Protection Condition ALPHA and BRAVO measures.
<input type="checkbox"/> <b>Measure 48.</b> Consider setting material condition ZEBRA, second deck and below.
<input type="checkbox"/> <b>Measure 49.</b> Cancel liberty. Execute emergency recall.
<input type="checkbox"/> <b>Measure 50.</b> Be prepared to get underway on short notice. If conditions warrant, request permission to sortie.
<input type="checkbox"/> <b>Measure 51.</b> Block all vehicle access to the pier.
<input type="checkbox"/> <b>Measure 52.</b> If the threat situation warrants, deploy picket boats to conduct patrols in the immediate vicinity of the ship. Brief boat crews and arm with appropriate weapons considering the threat, the local environment, and fields of fire.
<input type="checkbox"/> <b>Measure 53.</b> Coordinate with host nation/local port authority to establish small boat exclusion zone.
<input type="checkbox"/> <b>Measure 54.</b> Deploy the SSDF to protect command structure and augment posted watches. Station the SSDF in positions that provide 360-degree coverage of the ship.
<input type="checkbox"/> <b>Measure 55.</b> Energize radar and/or sonar, rotate screws and cycle rudder(s) at frequent and irregular intervals, as needed to assist in deterring, detecting or thwarting an attack.
<input type="checkbox"/> <b>Measure 56.</b> Consider manning repair locker(s). Be prepared to man one repair locker on short notice. Ensure adequate lines of communication are established with Damage Control Central.
<input type="checkbox"/> <b>Measure 57.</b> If available and feasible, consider use of airborne assets as an observation/force protection platform.
<input type="checkbox"/> <b>Measure 58.</b> If a threat of swimmer attack exists, activate an anti-swimmer watch.
<input type="checkbox"/> <b>Measure 59.</b> If unable to get underway, consider requesting augmentation.
<input type="checkbox"/> <b>Measure 60.</b> Review individual actions in Force Protection Condition DELTA for implementation.

**d. Force Protection Condition DELTA.** Declare Force Protection Condition DELTA when a terrorist attack has occurred in the immediate area or intelligence has been received that indicates a terrorist action against a specific location or person is likely. Normally, this Force Protection Condition is declared as a localized warning.

<input type="checkbox"/> <b>Measure 61.</b> Maintain appropriate Force Protection Condition ALPHA, BRAVO, and CHARLIE measures.
<input type="checkbox"/> <b>Measure 62.</b> Permit only necessary personnel topside.
<input type="checkbox"/> <b>Measure 63.</b> If possible, cancel port visit and get underway.
<input type="checkbox"/> <b>Measure 64.</b> Employ all necessary weaponry to defend against attack.

**FOR OFFICIAL USE ONLY****4. NONCOMBATANT SHIPBOARD FORCE PROTECTION CONDITIONS.**

**a. Force Protection Condition ALPHA.** Declare Force Protection Condition ALPHA when a general threat of possible terrorist activity is directed toward installations and personnel, the nature and extent of which are unpredictable, and where circumstances do not justify full implementation of Force Protection Condition BRAVO measures. However, it may be necessary to implement certain selected measures from Force Protection Condition BRAVO as a result of intelligence received or as a deterrent. Ships must be capable of maintaining Force Protection Condition ALPHA indefinitely.

<input type="checkbox"/> <b>Measure 1.</b> Brief crew on the port specific threat, the security/force protection plan, and security precautions to be taken while ashore. Ensure all hands are knowledgeable of various Force Protection Condition requirements and that they understand their role in implementation of measures.
<input type="checkbox"/> <b>Measure 2.</b> Muster and brief security personnel on the threat and rules of engagement.
<input type="checkbox"/> <b>Measure 3.</b> Review security plans and keep them available. Whenever possible, retain key personnel who may be needed to implement security measures on call.
<input type="checkbox"/> <b>Measure 4.</b> Secure spaces not in use and periodically inspect them.
<input type="checkbox"/> <b>Measure 5.</b> Remind all personnel to be suspicious and inquisitive of strangers, be alert for abandoned parcels or suitcases and for unattended vehicles in the vicinity. Report unusual activities to the master or mate on watch.
<input type="checkbox"/> <b>Measure 6.</b> Review pier and shipboard access control procedures.
<input type="checkbox"/> <b>Measure 7.</b> Ensure mate on watch, roving patrols and the gangway watch have the ability to communicate with one another.
<input type="checkbox"/> <b>Measure 8.</b> Coordinate pier/fleet landing security requirements with SOPA, collocated forces, and/or husbanding contractor. Identify anticipated needs for mutual support and define methods of activation and communication.
<input type="checkbox"/> <b>Measure 9.</b> Request husbanding contractor arrange and deploy barriers to keep vehicles away from the ship, if possible (400 feet minimum stand-off distance) consistent with threat.
<input type="checkbox"/> <b>Measure 10.</b> Randomly inspect hand carried items and packages before they are brought aboard.
<input type="checkbox"/> <b>Measure 11.</b> Regulate shipboard lighting to best meet the threat environment.
<input type="checkbox"/> <b>Measure 12.</b> Rig hawsepipe covers and rat guards on lines, cables and hoses. Consider using an anchor collar.
<input type="checkbox"/> <b>Measure 13.</b> Raise accommodation ladders, stern gates, ladders, etc. when not in use.
<input type="checkbox"/> <b>Measure 14.</b> Increase frequency of security drills.
<input type="checkbox"/> <b>Measure 15.</b> Review individual actions in Force Protection Condition BRAVO for possible implementation.

**b. Force Protection Condition BRAVO.** Declare Force Protection Condition BRAVO when an increased and more predictable threat of terrorist activity exists. The measures in this Force Protection Condition must be capable of being maintained for

**FOR OFFICIAL USE ONLY**

weeks without causing undue hardships, without affecting operational capability, and without aggravating relations with local authorities.

<input type="checkbox"/> <b>Measure 16.</b> Maintain appropriate Force Protection Condition ALPHA measures.
<input type="checkbox"/> <b>Measure 17.</b> Secure all watertight doors and hatches main deck and below.
<input type="checkbox"/> <b>Measure 18.</b> Consistent with local rules, regulations, and/or the Status of Forces Agreement, post pier sentries as necessary.
<input type="checkbox"/> <b>Measure 19.</b> Restrict vehicle access to the pier. Discontinue parking on the pier. Consistent with local rules, regulations, and/or the status of forces agreement, establish unloading zone(s) and move all containers as far away from the ship as possible (400 feet minimum stand-off distance) consistent with the threat.
<input type="checkbox"/> <b>Measure 20.</b> Post additional watches, as necessary.
<input type="checkbox"/> <b>Measure 21.</b> Post signs in local language that clearly define visiting and loitering restrictions.
<input type="checkbox"/> <b>Measure 22.</b> Identify and randomly inspect authorized watercraft daily, i.e. workboats, ferries and liberty launches.
<input type="checkbox"/> <b>Measure 23.</b> Direct liberty launches to make a security tour around the ship upon departure and arrival with particular focus on the waterline.
<input type="checkbox"/> <b>Measure 24.</b> Inspect all hand carried items, and packages before allowing them aboard. Where available, use baggage scanners and walk through or hand held metal detectors to screen packages and personnel prior to boarding the ship.
<input type="checkbox"/> <b>Measure 25.</b> Implement measures to keep unauthorized craft away from the ship. Coordinate with husbanding contractor and port authority as necessary.
<input type="checkbox"/> <b>Measure 26.</b> Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.
<input type="checkbox"/> <b>Measure 27.</b> Review liberty policy in light of the threat and revise it, as necessary, to maintain safety and security of ship and crew.
<input type="checkbox"/> <b>Measure 28.</b> Provide watchstanders daily threat updates.
<input type="checkbox"/> <b>Measure 29.</b> Master maintains a crew listing of all bilingual personnel for the area of operations. Ensure a warning tape or other suitable media is on the bridge that warns small craft to remain clear of ship. Warning should be in the local language and English. Maintain capability to broadcast warning on an announcing system.
<input type="checkbox"/> <b>Measure 30.</b> Arm the gangway or mate on watch.
<input type="checkbox"/> <b>Measure 31.</b> Review procedures for expedient issue of firearms and ammunition to the reaction force as deemed necessary by the master.
<input type="checkbox"/> <b>Measure 32.</b> Test internal and external communications. Include connectivity checks with local operational commander and authorities that will be expected to provide support, if required.
<input type="checkbox"/> <b>Measure 33.</b> Instruct watches to conduct frequent, random searches of pier to include pilings and access points.
<input type="checkbox"/> <b>Measure 34.</b> Conduct visual inspections of the ship's hull and ship's boats at intermittent intervals and immediately before getting underway.
<input type="checkbox"/> <b>Measure 35.</b> Hoist ships boats aboard when not in use.
<input type="checkbox"/> <b>Measure 36.</b> Terminate all public visits.

**FOR OFFICIAL USE ONLY**

<input type="checkbox"/> <b>Measure 37.</b> After working hours, reduce entry to ships interior by securing infrequently used entrances.
<input type="checkbox"/> <b>Measure 38.</b> Use only one gangway to access ship.
<input type="checkbox"/> <b>Measure 39.</b> Maintain capability to get underway on short notice or as specified by SOPA.
<input type="checkbox"/> <b>Measure 40.</b> Consider layout of fire hoses. Brief crew on procedures for repelling boarders, small boats, and ultra-light aircraft.
<input type="checkbox"/> <b>Measure 41.</b> Where possible, obstruct possible helicopter landing areas.
<input type="checkbox"/> <b>Measure 42.</b> Where possible, monitor local communications (ship to ship, TV, radio, police scanners, etc.).
<input type="checkbox"/> <b>Measure 43.</b> Inform local authorities of actions being taken as Force Protection Condition increases.
<input type="checkbox"/> <b>Measure 44.</b> Review individual actions in Force Protection Condition CHARLIE for possible implementation.

**c. Force Protection Condition CHARLIE.** Declare Force Protection Condition CHARLIE when an incident occurs or intelligence is received indicating that some form of terrorist action against installations and personnel is imminent. Implementation for more than a short period will probably create hardship, affecting the peacetime activities of the ship and its personnel.

<input type="checkbox"/> <b>Measure 45.</b> Maintain appropriate Force Protection Condition ALPHA and BRAVO measures.
<input type="checkbox"/> <b>Measure 46.</b> Consider securing all access doors and hatches main deck and below.
<input type="checkbox"/> <b>Measure 47.</b> Cancel liberty. Execute emergency recall.
<input type="checkbox"/> <b>Measure 48.</b> Prepare to get underway on short notice. If conditions warrant, request permission to sortie.
<input type="checkbox"/> <b>Measure 49.</b> Request armed security augmentation force.
<input type="checkbox"/> <b>Measure 50.</b> Coordinate with husbanding agent and/or local authorities to establish small boat exclusion zone around ship.
<input type="checkbox"/> <b>Measure 51.</b> Energize radar and/or sonar, rotate screws and cycle rudder(s) at frequent and irregular intervals, as needed to assist in deterring, detecting or thwarting an attack.
<input type="checkbox"/> <b>Measure 52.</b> Consider manning repair lockers. Be prepared to man one repair locker on short notice. Ensure adequate lines of communication are established with damage control central or equivalent location.
<input type="checkbox"/> <b>Measure 53.</b> If a threat of swimmer attack exists, activate an anti-swimmer watch.
<input type="checkbox"/> <b>Measure 54.</b> Review individual actions in Force Protection Condition DELTA for implementation.

**d. Force Protection Condition DELTA.** Declare Force Protection Condition DELTA when a terrorist attack has occurred in the immediate area or intelligence has been received that indicates a terrorist action against a specific location or person is likely. Normally, this Force Protection Condition is declared as a localized warning.

**FOR OFFICIAL USE ONLY**

- |   |
|---|
| <input type="checkbox"/> <b>Measure 55.</b> Maintain appropriate Force Protection Condition ALPHA, BRAVO, and CHARLIE measures. |
| <input type="checkbox"/> <b>Measure 56.</b> If possible, cancel port visit and get underway.                                    |
| <input type="checkbox"/> <b>Measure 57.</b> Employ all necessary weaponry to defend against attack.                             |

**5. AVIATION FACILITY FORCE PROTECTION CONDITION PROCEDURES**

**a. General.** In addition to basic Force Protection Condition procedures, units may need to perform a variety of other tasks at aviation facilities. This is particularly true for airbases located in areas where the threat of terrorist attacks is high.

**b. Force Protection Conditions ALPHA AND BRAVO****(1) Planning**

- |   |
|---|
| <input type="checkbox"/> Review Force Protection Conditions ALPHA and BRAVO measures.             |
| <input type="checkbox"/> Update Force Protection Conditions ALPHA and BRAVO measures as required. |

**(2) Briefing and Liaison**

- |   |
|---|
| <input type="checkbox"/> Brief all personnel on the threat, especially pilots, ground support crews, and air traffic controllers.             |
| <input type="checkbox"/> Inform local police of the threat. Coordinate plans to safeguard aircraft flight paths into and out of air stations. |
| <input type="checkbox"/> Ensure duty officers are always available by telephone.  |
| <input type="checkbox"/> Prepare to activate contingency plans and issue detailed air traffic control procedures if appropriate.              |
| <input type="checkbox"/> Be prepared to receive and direct aircraft from other stations.  |

**(3) Precautions Inside the Perimeter**

- |   |
|---|
| <input type="checkbox"/> Perform thorough and regular inspections of areas within the perimeters from which attacks on aircraft can be made.                            |
| <input type="checkbox"/> Take action to ensure no extremists armed with surface-to-air missiles can operate against aircraft within the perimeter.                      |
| <input type="checkbox"/> Establish checkpoints at all entrances and inspect all passes and permits. Identify documents of individuals entering the area--no exceptions. |
| <input type="checkbox"/> Search all vehicles, briefcases, packages, etc., entering the area.  |
| <input type="checkbox"/> Erect barriers around potential targets if at all possible.  |
| <input type="checkbox"/> Maintain firefighting equipment and conduct practice drills.   |
| <input type="checkbox"/> Hold practice alerts within the perimeter.   |

**(4) Precautions Outside the Perimeter**

- |   |
|---|
| <input type="checkbox"/> Conduct, with local host nation police or military authorities (as appropriate), regular |
|---|

C-2-A-14

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

inspections of the perimeter - especially the area adjacent to flight paths.
<input type="checkbox"/> Advise the local host nation authorities of any areas outside the perimeter where attacks could be mounted and which cannot be avoided by aircraft on takeoff or landing (when appropriate).
<input type="checkbox"/> Advise aircrews to report any unusual activity near approach and overshoot areas.

**c. Force Protection Condition CHARLIE****(1) Planning**

<input type="checkbox"/> Review Force Protection Condition CHARLIE measures.
<input type="checkbox"/> Update Force Protection Condition CHARLIE measures as required.

**(2) Briefing and Liaison**

<input type="checkbox"/> Brief all personnel on the increased threat.
<input type="checkbox"/> Inform local host nation authorities of increased threat.
<input type="checkbox"/> Coordinate with the local host nation authorities on any precautionary measures taken outside the airfield's perimeters.
<input type="checkbox"/> Implement appropriate flying countermeasures specified in SOPs when directed by air traffic controllers.

**(3) Precautions Inside the Perimeter**

<input type="checkbox"/> Inspect all vehicles and buildings on a regular basis.
<input type="checkbox"/> Detail additional guards to be on call at short notice and consider augmenting fire fighting details.
<input type="checkbox"/> Carry out random patrols within the airfield perimeter and maintain continuous observation of approach and overshoot areas.
<input type="checkbox"/> Reduce flying to essential operational flights only. Cease circuit flying if appropriate.
<input type="checkbox"/> Escort all visitors.
<input type="checkbox"/> Close relief landing grounds where appropriate.
<input type="checkbox"/> Check airfield diversion state.

**(4) Precautions Outside the Perimeter**

<input type="checkbox"/> Be prepared to react to requests for assistance.
<input type="checkbox"/> Provide troops to assist local host nation authorities in searching for terrorists on approaches outside the perimeter of military airfields.

**d. Force Protection Condition DELTA****(1) Planning**

**FOR OFFICIAL USE ONLY**

- |  |
|--|
| <input type="checkbox"/> Review Force Protection Condition DELTA measures.             |
| <input type="checkbox"/> Update Force Protection Condition DELTA measures as required. |

**(2) Briefings and Liaison**

- |  |
|--|
| <input type="checkbox"/> Brief all personnel on the very high levels of threat.        |
| <input type="checkbox"/> Inform local host nation authorities of the increased threat. |

**(3) Precautions Inside the Perimeter**

- |   |
|---|
| <input type="checkbox"/> Cease all flying except for specifically authorized operational sorties.   |
| <input type="checkbox"/> Implement, if necessary, appropriate flying countermeasures.   |
| <input type="checkbox"/> Be prepared to accept aircraft diverted from other stations.   |
| <input type="checkbox"/> Be prepared to deploy light aircraft and helicopters for surveillance tasks or to move internal security forces. |

**(4) Precautions Outside the Perimeter.** Close military roads allowing access to the airbase.



**FOR OFFICIAL USE ONLY****TAB B (NON-CONTROLLED/OFF-INSTALLATION FACILITY SECURITY STRATEGY) TO APPENDIX 2 (TERRORIST FORCE PROTECTION CONDITIONS) TO ANNEX C (OPERATIONS) TO USCINCEUR AT/FP OPORD 01-01**

**1. PURPOSE.** The intent of this Tab is to provide a strategy to address potential vulnerabilities found at activities/facilities outside the “protective security envelope” of a controlled entry, fenced military installation, e.g., Government-owned or -leased Housing/DODEA schools/AAFES or commissary complexes/isolated activity buildings. Commanders should consider these measures when developing local installation Force Protection Condition measures and physical security plans.

**2. CONCEPT.** Commanders can increase security and reduce the opportunity for a hostile agent to exploit known vulnerabilities by implementing some low cost procedures as well as applying programmatic solutions. Prior to implementing any of these strategies commanders should review existing assessment reports or conduct a supplemental Vulnerability Assessment to identify the most vulnerable points of a given facility.

**3. LOW COST/PROCEDURAL MEASURES**

<input type="checkbox"/> Establish regular high visibility security patrols of the facilities (should, if possible, include host nation assets).
<input type="checkbox"/> Conduct increased Random Antiterrorism Measures (RAM) in and around these facilities (check points/vehicle searches/Military Working Dogs). <b>On a frequent and/or daily basis, implement one or more Random Antiterrorism Measures (RAM) as a deterrent.</b> Increase the frequency, quantity and duration of RAMs in FPCON Bravo and Charlie.
<input type="checkbox"/> Increase the awareness of members living and working in these facilities (Town Hall meetings/local media/Command Info channels).
<input type="checkbox"/> Initiate a Neighborhood Watch program focused on AT/FP awareness. Example: If a suspicious person and or vehicle enters the housing area, Neighborhood Watch member would immediately notify their local Security Forces/Military Police (SF/MP).
<input type="checkbox"/> Reward Neighborhood Watch members for program participation —AAFES discounts (movie tickets, free bowling, etc.).
<input type="checkbox"/> Establish a community oriented policing program to bring SF/MP into a close working relationship with the Neighborhood Watch. SF/MP need to know who lives and works there. Likewise, Neighborhood Watch members need to feel comfortable about either discussing potential security problems with or making recommendations to SF/MP.
<input type="checkbox"/> If possible, have the SF/MP member assigned to monitor the housing area live in the housing area.
<input type="checkbox"/> Conduct building emergency action drills / individual action drills.
<input type="checkbox"/> <b>Protect off-installation military personnel and military transport in accordance with prepared plans. Remind drivers to lock parked vehicles and to check before entering or exiting the vehicle.</b>

**C-2-B-1****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

<input type="checkbox"/> Conduct mass notification exercises (announced/unannounced).
<input type="checkbox"/> Implement vehicle parking permit system—to assist the Security Force and Neighborhood Watch to quickly ID potential security risks.
<input type="checkbox"/> Train personnel to seek cover away from windows and into the most secure rooms in the facility.

**4. PHYSICAL SECURITY MEASURES (FUNDING REQUIRED)**

<input type="checkbox"/> Install security/vehicle barriers at “Key” vulnerability points to limit the vehicle access and increase the stand-off for the facilities—where possible limit close proximity parking.
<input type="checkbox"/> Apply fragmentation retention film (FRF) and window catch bars (blast mitigation systems) on windows that are directly exposed to uncontrolled close proximity vulnerable points.
<input type="checkbox"/> Install substantial security doors on all external entry ways. Ensure these doors open outward.
<input type="checkbox"/> Ensure entry points to all facilities are secured—master key access only. Advise family members to check home deliveries. Consider limiting times for delivery vehicles to enter the installations to maximize use of explosive detector dog teams and/or vehicle search teams.
<input type="checkbox"/> Install intercom building access systems
<input type="checkbox"/> Install mass notification systems for clustered housing areas.
<input type="checkbox"/> Install Closed Circuit Television (CCTV) camera coverage at key vulnerability points.
<input type="checkbox"/> Improve Security lighting
<input type="checkbox"/> Install Security Fencing, or at a minimum, triple strand concertina wire.

**5. LONG TERM SOLUTIONS.** If the facility has significant vulnerabilities and no cost-effective means of mitigation can be identified (such as those listed in paragraphs 3 and 4, above), commanders must work to either secure the facility (e.g., erect fences, install gates, post guards, etc.) or relocate the activity to a more secure location.

## FOR OFFICIAL USE ONLY

### TAB C (PROCEDURES FOR USE OF DEADLY FORCE) TO APPENDIX 2 (TERRORIST FORCE PROTECTION CONDITIONS) TO ANNEX C (OPERATIONS) TO USCINCEUR AT/FP OPORD 01-01

<b>REFERENCES:</b>	DoD Directive 5210.56, Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties, with Change 1, Feb 92
--------------------	--

1. The information in this Tab is taken from Enclosure 2 to DoDD 5210.56, and provides the requirements and procedures governing the use of deadly force. The information should be included in a "Use of Deadly Force" brief to all personnel performing law enforcement or guard duty. A "Use of Deadly Force" and/or Rules of Engagement (ROE) briefing is required when engaging in various missions, and explicitly when implementing Force Protection Condition BRAVO Measure 26. Security augmenters performing AT/FP operations to protect personnel, equipment, installations or activities should either be armed or have armed over-watch.
2. Service component commands may impose further restrictions on the use of deadly force if deemed necessary in their judgment, providing that such restrictions are consistent with Status of Forces Agreements (SOFA) and will not unduly compromise the national security interests of the United States.
3. Deadly force is justified only under conditions of extreme necessity and as a last resort when all lesser means have failed or cannot reasonably be employed. Deadly force is justified under one or more of the following circumstances:
  - a. Self-Defense and Defense of Others. When deadly force reasonably appears to be necessary to protect law enforcement or security personnel who reasonably believe themselves or others to be in imminent danger of death or serious bodily harm.
  - b. Assets Involving National Security. When deadly force reasonably appears necessary to prevent the actual theft or sabotage of assets vital to national security. DoD assets shall be specifically designated as "vital to national security" only when their loss, damage, or compromise would seriously jeopardize the fulfillment of a national defense mission. Examples include nuclear weapons; nuclear command, control, and communications facilities; and designated restricted areas containing strategic operational assets, sensitive codes, or special access programs.
  - c. Assets Not Involving National Security But Inherently Dangerous To Others. When deadly force reasonably appears to be necessary to prevent the actual theft or sabotage of resources, such as operable weapons or ammunition, that are inherently dangerous to others; i.e., assets that, in the hands of an unauthorized individual, present a substantial potential danger of death or serious bodily harm to others. Examples include high risk portable and lethal missiles, rockets, arms, ammunition, explosives, chemical agents, and special nuclear material.

## FOR OFFICIAL USE ONLY

**d. Serious Offenses Against Persons.** When deadly force reasonably appears necessary to prevent the commission of a serious offense involving violence and threatening death or serious bodily harm. Examples include murder, armed robbery, and aggravated assault.

**e. Arrest or Apprehension.** When deadly force reasonably appears to be necessary to arrest, apprehend, or prevent the escape of a person who, there is probable cause to believe, has committed an offense of the nature specified in subparagraphs 3b through 3d, above.

**f. Escapes.** When deadly force has been specifically authorized by the Heads of the DoD Components and reasonably appears to be necessary to prevent the escape of a prisoner, provided law enforcement or security personnel have probable cause to believe that the escaping prisoner poses a threat of serious bodily harm either to security personnel or others.

**4.** For contract security forces, use of the deadly force criteria shall be established consistent with this Tab and local law.

**5.** Personnel shall not be permitted to perform law enforcement or security duties requiring the use of weapons until they have received instruction on applicable regulations for the use of deadly force in the performance of such duties.

**6.** Additionally, annual refresher training shall be given to all personnel assigned to those duties to ensure that they continue to be thoroughly familiar with all restrictions on the use of deadly force.

**7.** Personnel carrying weapons for personal protection under the provisions Annex M, Appendix 4 shall have the necessary training on deadly force commensurate with that prescribed by this Tab.

**8.** Additional requirements for the use of firearms:

**a.** Warning shots are prohibited. *Unless otherwise mandated in a particular country by the SOFA.*

**b.** 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 prompting the individual to shoot.

**c.** Shots shall be fired only with due regard for the safety of innocent bystanders.

**d.** In the case of holstered weapons, a weapon should not be removed from the holster unless there is reasonable expectation that use of the weapon may be necessary.

**C-2-C-2**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**e.** Service component commanders may establish additional considerations in implementing procedures over the use of firearms.

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**C-2-C-4**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### APPENDIX 3 (WEAPONS OF MASS DESTRUCTION (WMD)) TO ANNEX C (OPERATIONS) TO USCINCEUR AT/FP OPOD 01-01

- REFERENCES:**
- a. FM 3-6/AFM 105-7/FMFM 7-11H, Field Behavior of Chemical Agents
  - b. FM 3-10-1/NWP 18-1/AFM 355-4/FMFM 7-11, Chemical Weapons Employment
  - c. FM 8-285/NAVMED P-541/AFM 160-11, Treatment of Chemical Agent Casualties and Conventional Military Chemical Injuries
  - d. FM 3-3, Chemical and Biological Contamination Avoidance
  - e. FM3-3-1, Nuclear Defense
  - f. FM 3-4, NBC Protection
  - g. FM 3-5, NBC Decontamination
  - h. FM 3-7, NBC Handbook
  - i. FM 3-100, NBC Defense, Chemical Warfare, and Smoke and Flame Operations
  - j. FM 8-10, Health Service Support in a Theater of Operations
  - k. FM 8-10-7, Health Service Support in a Nuclear, Biological, and Chemical Environment
  - l. NSTM, Chapter 070, Shipboard Radiological Defense
  - m. NSTM, Chapter 470, Shipboard BW/CW Defense and Countermeasures
  - n. NBC, Warfare Defense Ashore
  - o. MCWP 3-37.2, NBC Protection
  - p. MCWP 3-37.3, NBC Decontamination
  - q. MCWP 3-37, MAGTF NBC Defense
  - r. MCWP 3-37.2A, Chemical and Biological Contamination Avoidance
  - s. MCWP 3-37.2B, Nuclear Contamination Avoidance
  - t. MCWP 3-37.4, NBC Reconnaissance
  - u. AFI 32-4001, Disaster Preparedness and Planning Operations
  - v. AFM 32-4005, Personnel Protection and Attack Actions
  - w. USEUCOM Directive 56-1, Nuclear Biological, and Chemical Defense; Riot Control Agents; Herbicides; and Non-Lethal Weapons (S)

**1. PURPOSE.** This Annex provides an overview of the potential use of WMD by terrorists and broad guidance implementing USEUCOM Prescriptive AT/FP Program

## FOR OFFICIAL USE ONLY

Standard 10 (see Annex M, Appendix 1). WMD include biological and chemical agents or material, plant and animal toxins, radiological material, nuclear devices, and high yield explosives used as weapons against personnel, animals, plants, material, or facilities.

### 2. WMD PLANNING CONSIDERATIONS

a. General. The threat of terrorist use of WMD poses great challenges for military organizations. Previous concerns regarding WMD use focused on battlefield employment against warned and protected military personnel. The threat has expanded in recent years as terrorist organizations have grown in sophistication and now have the ability to acquire and employ WMD. This growing threat now means units must plan for the possible use of WMD against peacetime forces and noncombatants.

b. Existing military doctrine addresses the use of chemical, biological, radiological, nuclear, and high yield explosive (CBRN-E) weapons and their effects on personnel and facilities. Planning factors for battlefield use of these weapons may have direct application when planning for terrorist use of WMD. A list of current publications that address CBRN-E weapons, their effects, and planning factors is provided as references in the Basic Order and this Appendix. Table C-3-1, below, summarizes planning considerations in existing doctrinal publications on the use of CBRN-E weapons.

**Table C-3-1: Doctrinal NBC Planning Considerations**

<b><u>Considerations</u></b>	<b><u>Include</u></b>
Contamination Avoidance	Contamination Control, Detection and Warning, Identification and Marking, and Passive Defense Measures
Protection	Individual Protection and Collective Protection
Decontamination	Immediate, Operational and Thorough Decontamination
Medical Aspects	Treatment; Intervention/Countermeasures; and Casualty Evacuation and Handling
Other Considerations	DoD Dependents, Civilians and Contractors; Host Nation and Multinational Forces and Personnel

### 3. POTENTIAL THREAT OF TERRORIST USE OF WMD

a. The potentially devastating effects of terrorist use of WMD mandates that organizations conduct a thorough analysis of the threat in their AOR. The unique aspects of the terrorist capability to acquire and employ WMD should be considered as a distinct element of the overall threat assessment.

b. The USEUCOM proponent for WMD efforts is ECJ5. ECJ2, in conjunction with ECJ5, will establish an integrated collection and analysis program that draws detailed threat data from all available sources to support command WMD efforts.

c. Collection plans should address the Essential Elements of Information (EEI) of the terrorist capability to acquire and use of WMD. EEIs should be integrated into

**C-3-2**

**FOR OFFICIAL USE ONLY**



## FOR OFFICIAL USE ONLY

subordinate elements' collection plans and reviewed as new or evolving threats emerge. The plan should consider terrorist threats from commercial, industrial and medical source material as well as traditional military CBRN-E weapons and agents.

**d.** New or changing terrorist capabilities to acquire or employ WMD must be rapidly disseminated through command channels. Units should include procedures for immediate reporting of changing terrorist threats or actual use of WMD. Notification should be sent through the chain of command as outlined in Annex C, Appendix 2.

#### 4. VULNERABILITY ASSESSMENTS OF TERRORIST USE OF WMD

**a.** Organizations will assess the vulnerability of installations, facilities, and personnel in their AOR to terrorist use of WMD. Vulnerability assessments will be based on the threat assessments and application of the guidance and procedures in Annex M, Appendix 2.

**b.** As a minimum, assessments should include information from intelligence, logistics, medical, physical security, facility engineering, meteorological, explosive ordnance disposal, and CBRN-E staff elements. The entire range of potential terrorist WMD use should be considered when conducting assessments. As previously mentioned, threats from commercial chemical, biological, nuclear, and radiological sources should be included as well as traditional military agents. Examples of possible vulnerabilities could include:

<input type="checkbox"/> Individual protective clothing and equipment
<input type="checkbox"/> Collective protection equipment and facilities
<input type="checkbox"/> Medical response and emergency services capability
<input type="checkbox"/> Training of personnel
<input type="checkbox"/> Physical security and protective barriers
<input type="checkbox"/> Facility design and construction
<input type="checkbox"/> Early warning and detection
<input type="checkbox"/> Alarms and attack warning
<input type="checkbox"/> Threat Intelligence
<input type="checkbox"/> Sustainment operations and follow on support
<input type="checkbox"/> Preventive medicine and vaccination programs
<input type="checkbox"/> Storage of bulk hazardous material
<input type="checkbox"/> Explosive ordnance disposal response capability/availability.

#### 5. CONSEQUENCE MANAGEMENT (MITIGATION OF TERRORIST USE OF WMD)

**a.** Units and installations will take appropriate measures to protect personnel and facilities and reduce their vulnerability to terrorist use of WMD. Mitigating the consequences of the actual terrorist use of WMD is critical to reducing the loss of life and property. This includes actions taken prior to use as well as actions taken subsequent to the attack. Actions may be physical security improvements such as

## FOR OFFICIAL USE ONLY

installing an integrated large area siren and warning system, or procedural improvements such as exercising and validating the WMD emergency response annex or plan.

**b.** As a part of the overall installation/activity AT/FP Plan, commanders should address the WMD threat and exercise the WMD part of the plan to determine its effectiveness in mitigating the effects of an attack. In addition to providing crisis action and consequence management procedures, planning should include pre-attack measures and consideration for the collateral damage WMD may have on adjacent facilities and surrounding communities. Plans should provide sufficient detail to permit organizations to rapidly recognize and respond to any terrorist event using WMD.

**c.** The following contains additional crisis action planning considerations that should be included in addressing terrorist use of WMD:

**(1) Commander's estimate of the potential for use of WMD:** This forms the basis for all facts and assumptions that drive the planning and preparation for any use of WMD by potential threat organizations. As such, the commander's estimate is the cornerstone of any successful program and must be reviewed frequently to incorporate any new or emerging threats.

**(2) Type/number of threats:** Accurate identification of the WMD threats posed by terrorist organizations provides a mechanism to determine the resources needed to counter the threat and respond effectively if they are used. Planners should also factor in the magnitude and diversity of the threats throughout an AOR.

**(3) Most likely/most vulnerable targets:** Most organizations can't provide total protection for all personnel and facilities in their AOR. However, identification of the most likely and vulnerable targets enables more detailed planning, which then drives responsible organizations to improve security measures. Further, responsible organizations can take measures to improve the security for these areas.

**(4) Target Value Analysis:** Certain areas pose different challenges due to their specific value to terrorists. These targets may not be mission related or of high military value, but their value to terrorists may be very high because of inherent vulnerabilities and the potential for mass casualties. High use areas, such as shopping facilities or office complexes, have inherent problems with access control and usually have large concentrations of unprotected personnel present. Special analysis and planning should be done to help reduce the vulnerability of these types of areas.

**(5) Coordination with local authorities:** Coordination with local authorities is essential when planning for terrorist WMD use. It is likely that an attack on either the DoD facility or the local civilian populace will affect both communities. Dispersion of the agent effects by environmental factors (wind, water, or animals) can quickly spread to surrounding areas. Thorough coordination between DoD organizations and local officials provides a means to improve the response time and offers the opportunity to

## FOR OFFICIAL USE ONLY

share critical resources needed to mitigate the effects of an attack. These arrangements should be formalized in Memoranda of Agreement with local officials.

**(6) Attack recognition and agent characterization:** Unless prior warning is obtained of an impending attack, most organizations will not have automatic detection devices and alarms in operation. Attack recognition may come only when symptoms first appear in exposed personnel. Agent identification will probably be done by first responders or medical personnel. Planning must address this potential vulnerability and incorporate procedures that include adequate training, individual protective equipment, and detection equipment for first responders, and minimize the delay from attack initiation until detection.

**(7) Warning systems:** Because WMD attacks can cover large areas, timely warning can reduce the number of personnel who would otherwise be exposed to agent effects. A combination of outdoor warning sirens, telephonic notification, and broadcast announcements provide redundant warning systems that will reach a large portion of the population. Special consideration should be given to unique populations, such as the visually or hearing impaired, to ensure effective warning systems are in place to provide for their safety.

**(8) Response levels:** Different agents require different responses. Plans should include details on the appropriate response for the agents identified in commander's assessment and the equipment needed to implement that level of response.

**(9) Hazardous Material Response Teams:** Host nation laws and directives may contain specific requirements for personnel responding to hazardous material and substances. Commanders must be aware of these requirements, and emergency responders must have the equipment and training necessary to protect themselves, treat casualties and decontaminate the site. Planning should include adequate time and resources to ensure response teams have the appropriate equipment and level of training.

**(10) Reporting procedures:** Because of the sensitivity of terrorist use of WMD, many agencies require formatted reports on the nature of the event. Plans should include pre-formatted templates for reporting requirements and message addresses and phone numbers for the agencies and commands that must be notified. Communications can rapidly overload available communications means during a crisis. Brevity codes, established crisis action communication procedures and predetermined local reporting requirements will all assist in the management of a crisis by providing timely and accurate information to the emergency operations center. The procedures for reporting terrorist incidents in Annex C, Appendix 2 should be used as a guide for reporting WMD incidents.

**(11) Crisis action team responsibilities:** Emergency operations centers normally have only a small staff on duty and will require immediate augmentation when an attack occurs. Staff elements should be fully trained and prepared to implement the

## FOR OFFICIAL USE ONLY

appropriate plan to reduce the effects of the WMD attack. It may be necessary to operate in protective equipment during the initial stages of the crisis. Training on the use of protective equipment and their specific duties as part of the emergency operations center staff should be regularly exercised to maintain proficiency in crisis action responsibilities.

**(12) First responder responsibilities:** First responders will be called on to perform many critical functions during a WMD attack. Law enforcement, fire, medical, explosive ordnance disposal and facility engineer teams will usually be some of the first organizations to react to an event. Careful planning and training is needed to address the special needs of these groups. The actions they take during the initial stages of an event will have a very important impact on the consequence management steps that follow.

**(13) Medical support, treatment and transportation requirements:** Prior coordination with host nation medical facilities is necessary to ensure medical plans include procedures to treat and care for contaminated or infected personnel. Medical teams require special training in the treatment and handling of contaminated casualties and remains. Medical facilities should have areas designated to treat and segregate contaminated patients. Preventive medicine specialists and pathologists need to have a database of naturally occurring diseases and procedures to quickly assess and identify suspicious illnesses and diseases. Antidotes and treatments for potential agents from commercial or industrial sources should be considered in the casualty management plan. Contaminated patient transport and contamination control measures should be incorporated into litter and ambulance operations.

**(14) Temporary Shelters, Evacuation routes and care centers:** There will always be a requirement to clear an area and provide orderly evacuation to safe areas when WMD is used. Temporary shelters, evacuation routes, and care centers should be identified during the planning process. Commanders should identify facilities for potential use in defense against chemical, radiological, and biological agents. Existing facilities may be suitable for adaptation as temporary shelters/toxic-free areas, since sufficient collective protection resources may be inadequate. Law enforcement and security personnel need to determine traffic control points to facilitate evacuation and prevent personnel from entering potentially contaminated areas. Copies of the routes and locations of care centers should be available to installation workers and residents.

**(15) Public affairs:** The demand for information from the public and the media will be intense at the onset of an event. Public affairs planning should include background information on the potential agents and materials that pose a threat. Basic information on the properties, effects, treatment, duration, and decontamination of likely threat agents should be included in the public affairs reference materials brought to the emergency operations center and joint information center. Rapid and accurate information on the hazard during the early stages of an event will assist in protecting civilians from hazard and foster confidence in the command's ability to safely manage the crisis.

## FOR OFFICIAL USE ONLY

**(16) Crime scene procedures for agent material:** Terrorist use of any WMD material is a criminal act. Local plans should include procedures to control a crime scene in a contaminated environment and provide for the recovery of evidence that may be hazardous. These plans also should include procedures that are required under host nation laws or status of forces agreements.

**(17) Follow on assistance:** Any WMD event may generate the requirement for some form of external support or assistance. Plans should determine the type, amount and time frame for follow-on assistance. The logistics of managing a large contingent of external support organizations has the potential of overwhelming the ability of the local commander to control its effective employment.

**(18) Hazard prediction:** When an event occurs, there is an immediate need to predict the size of the potential hazard zone. Reports from first responders will contain the location of the incident site; but the initial estimate of the hazard area should be made by emergency operations center personnel. Procedures should be incorporated into emergency operations centers that allow for a quick initial hazard prediction and methods for its rapid dissemination. Detailed predictions can be made when more information is provided on the agent type and dissemination means.

**(19) Meteorological support:** As indicated above, hazard prediction must be done quickly. Current and reliable weather data is critical to providing accurate hazard predictions. Updated weather data should be routinely provided to emergency operations centers so that it is available at the onset of an event. Organizations providing data should be part of the planning process so they can develop weather products that support hazard prediction models or programs.

**(20) Contamination control:** Containing and limiting the spread of contamination is essential in reducing the effects of a WMD attack. Procedures for personnel responding to the attack site should include methods that minimize their direct contact with contaminated material. Work crews should use sumps to collect runoff from decontamination operations. Access into the site should be through designated points and along designated routes.

**(21) Decontamination and hot line operations:** Decontamination procedures should be developed using the resources locally available. Decontaminating exposed personnel, first responders, and site work teams requires the rapid establishment of a decontamination site. Plans should consider the requirement to maintain decontamination operations for extended periods and the potentially large personnel and logistics need generated to support this type of operation.

**(22) Sampling and analysis:** Sampling will be required at the attack site and in the predicted hazard areas to establish the presence or absence of contamination. Plans should include procedures to determine sampling requirements and protocols for the collection of agent material, to include procedures for maintaining a chain of

## FOR OFFICIAL USE ONLY

custody. Analysis of samples may be done locally at the onset of an attack, but may be shipped off-site for confirmation or for detailed analysis if local facilities cannot identify the material.

**(23) Monitoring operations:** Monitoring plans should include procedures to deploy detection equipment to known or suspected hazard locations. Detection equipment intended for military tactical level employment does not detect agent concentrations that are considered hazardous by the EPA and the Occupational Safety and Health Administration. Environmental and safety planners must be aware of the hazardous material exposure limits for civilian populations and understand the limitations of using military equipment to determine when areas are considered free of contamination.

**(24) Reentry and remediation operations:** Preliminary planning should address the considerations for these operations. Reentry includes actions required to permit personnel to safely enter an area following an attack. Remediation includes actions to remove all contamination from the site and restore the environment to its original condition. Both of these processes can potentially take several days to weeks to complete. External support will probably be needed to ensure these tasks are properly accomplished.

**(25) Training Requirements:** Training programs should provide a comprehensive approach to meeting the needs identified in mitigation efforts. Actions required to reduce the vulnerability to attack and to respond as the result of a terrorist WMD incident involve many different tasks and levels of training. At a minimum, training programs should include individual, first responder, functional response team, and emergency operations center training.

### Mitigation and Consequence Management Guidelines Checklist ( To Assist in Planning For Terrorist Use of WMD)

<input type="checkbox"/> 1. <b>Pre-deployment and garrison operations.</b>
<input type="checkbox"/> a. Command, control, communications, computers, and intelligence (C4I):
<input type="checkbox"/> Review and update operational plans based on probable threats.
<input type="checkbox"/> b. Active defense (as defined in Joint Pub 1-02, 12 Apr 01):
<input type="checkbox"/> Gather intelligence on potential terrorist capability.
<input type="checkbox"/> Identify essential elements of enemy information on terrorist capability.
<input type="checkbox"/> c. Detection and Identification:
<input type="checkbox"/> Gather meteorological data for area of operations.
<input type="checkbox"/> Gather intelligence regarding terrorist WMD capabilities.
<input type="checkbox"/> Conduct refresher training on all detection equipment.
<input type="checkbox"/> Identify threats that require laboratory analysis for identification.
<input type="checkbox"/> Develop specific identification techniques and acquire materials to conduct analysis.
<input type="checkbox"/> d. Hazard prediction, warning, and reporting:

## FOR OFFICIAL USE ONLY

<ul style="list-style-type: none"><li><input type="checkbox"/> Conduct training for all personnel in the warning and reporting chain.</li><li><input type="checkbox"/> Exercise the warning and reporting system and communications nets.</li><li><input type="checkbox"/> Identify hazard prediction models and exercise procedures.</li></ul>
<input type="checkbox"/> e. Reconnaissance, survey, and monitoring:
<ul style="list-style-type: none"><li><input type="checkbox"/> Develop sample collection, packaging, transportation, documentation, and analysis procedures.</li><li><input type="checkbox"/> Conduct training for reconnaissance and survey teams.</li><li><input type="checkbox"/> Identify laboratory locations to support agent identification.</li></ul>
<input type="checkbox"/> f. Individual Protection:
<ul style="list-style-type: none"><li><input type="checkbox"/> Conduct training for individual defensive procedures and equipment use.</li><li><input type="checkbox"/> Issue individual equipment as appropriate.</li><li><input type="checkbox"/> Stockpile replacement items.</li></ul>
<input type="checkbox"/> g. Collective protection:
<ul style="list-style-type: none"><li><input type="checkbox"/> Identify and quantify requirements.</li><li><input type="checkbox"/> Identify facilities that may be used as toxic-free areas.</li><li><input type="checkbox"/> Conduct operational checks of on-hand collective protection equipment.</li><li><input type="checkbox"/> Stockpile replacement items.</li></ul>
<input type="checkbox"/> h. Medical:
<ul style="list-style-type: none"><li><input type="checkbox"/> Conduct medical threat analysis.</li><li><input type="checkbox"/> Provide medical input to medical force development planning.</li><li><input type="checkbox"/> Train in medical aspects of WMD defense.</li><li><input type="checkbox"/> Review medical logistics support.</li><li><input type="checkbox"/> Implement vaccination policy.</li><li><input type="checkbox"/> Review individual procedures for hygiene in a contaminated environment.</li><li><input type="checkbox"/> Review individual/collective procedures for defense by medical units against WMD.</li></ul>
<input type="checkbox"/> i. Contamination control:
<ul style="list-style-type: none"><li><input type="checkbox"/> Identify assets and rehearse procedures.</li></ul>
<input type="checkbox"/> j. Logistics:
<ul style="list-style-type: none"><li><input type="checkbox"/> Review planning factors for operations in contaminated environment.</li><li><input type="checkbox"/> Identify resources to support sustained operations in contaminated environment.</li><li><input type="checkbox"/> Identify resource shortfalls, e.g., personnel, equipment, funding, training, etc., and report these program weaknesses to higher headquarters.</li></ul>
<input type="checkbox"/> <b>2. Pre-attack procedures.</b>
<input type="checkbox"/> a. C4I:
<ul style="list-style-type: none"><li><input type="checkbox"/> Pre-plan for WMD event.</li><li><input type="checkbox"/> Issue mission orders and directives.</li><li><input type="checkbox"/> Activate WMD reporting chain.</li><li><input type="checkbox"/> Order appropriate WMD protective actions and posture.</li><li><input type="checkbox"/> Enforce counter-surveillance measures.</li><li><input type="checkbox"/> Coordinate with local civilian or host nation governments.</li></ul>
<input type="checkbox"/> b. Active defense (as defined in Joint Pub 1-02, 12 Apr 01):
<ul style="list-style-type: none"><li><input type="checkbox"/> Allocate resources to active defense mission.</li><li><input type="checkbox"/> Monitor terrorist offensive actions.</li><li><input type="checkbox"/> Disrupt terrorist planning cycle and C4I means.</li></ul>

## FOR OFFICIAL USE ONLY

<input type="checkbox"/> c. Detection and identification:
<input type="checkbox"/> Conduct routine background analysis and periodic monitoring.
<input type="checkbox"/> Conduct refresher training for detector operators.
<input type="checkbox"/> Position detectors.
<input type="checkbox"/> d. Warning and reporting:
<input type="checkbox"/> Conduct refresher training in WMD warning and reporting.
<input type="checkbox"/> Initiate and maintain disease and non-battle injury reporting system.
<input type="checkbox"/> e. Reconnaissance, survey, and monitoring:
<input type="checkbox"/> Position assets.
<input type="checkbox"/> Stockpile sample collection and transportation equipment.
<input type="checkbox"/> Stockpile agent identification equipment.
<input type="checkbox"/> Conduct routine sampling in accordance IAW the threat and detector capabilities.
<input type="checkbox"/> f. Individual protection:
<input type="checkbox"/> Implement unit standard operating procedures for WMD Operations.
<input type="checkbox"/> Adopt protective level appropriate to the threat.
<input type="checkbox"/> Prepare to take additional protective measures when warned of possible or actual attack.
<input type="checkbox"/> g. Collective protection:
<input type="checkbox"/> Post sentries on entrance to collective protection shelters.
<input type="checkbox"/> Adopt increasingly defensive posture in line with threat level.
<input type="checkbox"/> h. Medical:
<input type="checkbox"/> Provide medical input to Commander's estimate of the threat.
<input type="checkbox"/> Review and promulgate medical treatment protocols.
<input type="checkbox"/> Identify specialist medical teams.
<input type="checkbox"/> i. Contamination control:
<input type="checkbox"/> Identify water sources and decontamination solutions.
<input type="checkbox"/> Position equipment and supplies.
<input type="checkbox"/> j. Logistics:
<input type="checkbox"/> Confirm availability of equipment and supplies for operations in a contaminated environment.
<input type="checkbox"/> Identify host nation, federal, state, or local resources that may be available to augment unit assets.
<input type="checkbox"/> <b>3. Actions during attack.</b>
<input type="checkbox"/> a. C4I:
<input type="checkbox"/> Transmit appropriate reports.
<input type="checkbox"/> Synthesize attack information.
<input type="checkbox"/> Notify local/host nation government.
<input type="checkbox"/> b. Active defense (as defined in Joint Pub 1-02, 12 Apr 01):
<input type="checkbox"/> Disrupt terrorist delivery systems.
<input type="checkbox"/> c. Detection and identification:



## FOR OFFICIAL USE ONLY

<ul style="list-style-type: none"><li><input type="checkbox"/> Collect samples.</li><li><input type="checkbox"/> Coordinate and analyze intelligence, meteorological, medical, and detector system input.</li><li><input type="checkbox"/> Prepare and forward samples to lab for further analysis and identification.</li><li><input type="checkbox"/> Conduct downwind hazard analysis and disseminate predictions.</li></ul>
<ul style="list-style-type: none"><li><input type="checkbox"/> d. Warning and reporting:<ul style="list-style-type: none"><li><input type="checkbox"/> Implement warning and reporting procedures.</li><li><input type="checkbox"/> Report and forward evidence of attack to command, medical and law enforcement authorities.</li><li><input type="checkbox"/> Make and disseminate alarm/protective action decisions.</li></ul></li></ul>
<ul style="list-style-type: none"><li><input type="checkbox"/> e. Reconnaissance, survey and monitoring:<ul style="list-style-type: none"><li><input type="checkbox"/> Implement collection and survey plans.</li><li><input type="checkbox"/> Collect any aerosol, environmental, plant/animal, and medical samples.</li><li><input type="checkbox"/> Report results of field surveys and monitoring efforts.</li></ul></li></ul>
<ul style="list-style-type: none"><li><input type="checkbox"/> f. Individual protection:<ul style="list-style-type: none"><li><input type="checkbox"/> Implement appropriate protection for personnel.</li><li><input type="checkbox"/> Implement evacuation plans for non-essential personnel and civilians.</li><li><input type="checkbox"/> Provide resupply of expended items and contaminated equipment.</li></ul></li></ul>
<ul style="list-style-type: none"><li><input type="checkbox"/> g. Collective protection:<ul style="list-style-type: none"><li><input type="checkbox"/> Activate collective protection shelters for key assets.</li><li><input type="checkbox"/> Maintain strict control over access to collective protection shelters.</li></ul></li></ul>
<ul style="list-style-type: none"><li><input type="checkbox"/> h. Medical:<ul style="list-style-type: none"><li><input type="checkbox"/> Initiate treatment of contaminated casualties.</li><li><input type="checkbox"/> Confirm detection system results.</li><li><input type="checkbox"/> Characterize agents.</li><li><input type="checkbox"/> Monitor outbreaks.</li><li><input type="checkbox"/> Maintain integrity of medical collective protection.</li></ul></li></ul>
<ul style="list-style-type: none"><li><input type="checkbox"/> i. Contamination control:<ul style="list-style-type: none"><li><input type="checkbox"/> Determine extent of attack location.</li><li><input type="checkbox"/> Control access to site and establish designated routes to and from the area.</li><li><input type="checkbox"/> Have first responders attempt to provide hasty decon of the known hazard area.</li><li><input type="checkbox"/> Implement decontamination plan.</li></ul></li></ul>
<ul style="list-style-type: none"><li><input type="checkbox"/> j. Logistics:<ul style="list-style-type: none"><li><input type="checkbox"/> Issue replacement items.</li><li><input type="checkbox"/> Replace expended supplies and contaminated items.</li></ul></li></ul>
<ul style="list-style-type: none"><li><input type="checkbox"/> <b>4. Post-attack actions.</b></li></ul>
<ul style="list-style-type: none"><li><input type="checkbox"/> a. C4I:<ul style="list-style-type: none"><li><input type="checkbox"/> Assess result of terrorist attack.</li><li><input type="checkbox"/> Assess terrorist intention for any further attacks.</li><li><input type="checkbox"/> Ensure continued operation of WMD warning and reporting system.</li><li><input type="checkbox"/> Update threat based on latest attack information.</li><li><input type="checkbox"/> Order implementation of specific post-attack control measures.</li><li><input type="checkbox"/> Identify resource and capability shortfalls.</li></ul></li></ul>

## FOR OFFICIAL USE ONLY

b. Active defense (as defined in Joint Pub 1-02, 12 Apr 01):
<ul style="list-style-type: none"><li><input type="checkbox"/> Target any residual capability.</li><li><input type="checkbox"/> Execute appropriate military response.</li></ul>
c. Detection and identification:
<ul style="list-style-type: none"><li><input type="checkbox"/> Relocate detectors to any predicted agent locations.</li><li><input type="checkbox"/> Continue sampling and monitoring until agent levels are below permissible exposure levels.</li></ul>
d. Warning and reporting:
<ul style="list-style-type: none"><li><input type="checkbox"/> Disseminate decisions on protection, hazard avoidance, and countermeasures.</li><li><input type="checkbox"/> Collect and forward casualty and disease reports.</li><li><input type="checkbox"/> Continue to report unexplained illnesses or agent symptoms.</li></ul>
e. Reconnaissance, survey and monitoring:
<ul style="list-style-type: none"><li><input type="checkbox"/> Identify contaminated areas for environmental remediation.</li><li><input type="checkbox"/> Continue to collect samples to verify initial results.</li><li><input type="checkbox"/> Provide agent samples to law enforcement authorities.</li></ul>
f. Individual protection:
<ul style="list-style-type: none"><li><input type="checkbox"/> Initiate controlled down dressing for protected personnel.</li><li><input type="checkbox"/> Redistribute supplies of individual equipment.</li></ul>
g. Collective protection:
<ul style="list-style-type: none"><li><input type="checkbox"/> Decontaminate as necessary.</li><li><input type="checkbox"/> Replace filters.</li></ul>
h. Medical:
<ul style="list-style-type: none"><li><input type="checkbox"/> Implement strict field hygiene measures.<ul style="list-style-type: none"><li><input type="checkbox"/> Review treatment protocols and agent symptoms.</li><li><input type="checkbox"/> Characterize outbreaks.</li><li><input type="checkbox"/> Deploy specialist teams.</li><li><input type="checkbox"/> Institute quarantine as necessary.</li><li><input type="checkbox"/> Document and treat casualties.</li><li><input type="checkbox"/> Analyze and distribute medical intelligence.</li><li><input type="checkbox"/> Ensure medical protective measures for follow-on support is complete.</li><li><input type="checkbox"/> Ensure safety of food and water supplies.</li></ul></li></ul>
i. Contamination Control:
<ul style="list-style-type: none"><li><input type="checkbox"/> Restrict movements of personnel and equipment into the hazard zone.</li><li><input type="checkbox"/> Establish multiple sites to speed the decontamination of personnel as appropriate.</li></ul>
j. Logistics:
<ul style="list-style-type: none"><li><input type="checkbox"/> Replenish contingency stocks.</li><li><input type="checkbox"/> Reissue decontaminated equipment.</li><li><input type="checkbox"/> Review accuracy of planning factors.</li></ul>

**FOR OFFICIAL USE ONLY**

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
**General, USAF**

**C-3-13**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**C-3-14**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### APPENDIX 4 (USDR SECURITY RESPONSIBILITIES AND PROCEDURES) TO ANNEX C (OPERATIONS) USCINCEUR AT/FP OPOD 01-01

<b>REFERENCES:</b>	<ul style="list-style-type: none"><li>a. Public Law 99-399, Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended</li><li>b. Section 4802 and 4805(A) of Title 22, United States Code</li><li>c. DOS, Volume 12, Foreign Affairs Manual (FAM 12)</li><li>d. DoD Instruction 5210.84, Security of DoD Personnel at U.S. Missions Abroad, 22 Jan 92</li><li>e. DoD Handbook 2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence, Sep 93 w/Change 2</li><li>f. DoD and DOS Memorandum of Understanding on Force Protection On Security of DoD Elements and Personnel In Foreign Areas, 16 Dec 97</li><li>g. DoD Instruction 5105.57, Procedures for the U.S. Defense Representative (USDR) in Foreign Countries, Dec 95</li><li>h. USEUCOM Directive 56-9, Procedures for the U.S. Defense Representative (USDR), Jun 98</li></ul>
--------------------	--

**1. SITUATION.** The U.S. Defense Representative (USDR) coordinates all Antiterrorism/Force Protection (AT/FP) matters of those DoD elements and personnel for whom the Chief of Mission (COM) has security responsibility, as stated in Section 4805, Title 22, and/or as defined in a Memorandum of Agreement (MOA) between the CINC and COM.<sup>1</sup>

**2. MISSION.** To provide AT/FP guidance regarding the responsibilities and authority of the USDR for DoD elements for whom the COM has security responsibility.

### **3. EXECUTION**

**a. Scheme of Support.** The USDR coordinates AT/FP with the COM, the Regional Security Officer (RSO), Post Security Officer (PSO), ECJ4 (for Turkey), ECJ5, and ECSM. This Appendix specifies the AT/FP duties of the USDR and provides guidance on the discharge of the USDR's assigned security duties, responsibilities and procedures. Department of State (DOS) uses the term "security" to describe those

---

<sup>1</sup> The USDR also serves as a focal point for DoD element commanders deploying to regions with a limited U.S. military presence. DoD element commanders/senior officers should contact the USDR prior to, or immediately upon arrival at the deployment location, to exchange information which may be beneficial to the USDR and/or DoD element.

## FOR OFFICIAL USE ONLY

functions and programs commonly encompassed by the DoD term "antiterrorism/ force protection (AT/FP)". The objectives and intent of both the DOS and DoD programs are essentially identical – to provide a safe and secure working and living environment for U.S. personnel.

### **b. Tasks to subordinate units**

#### **(1) HQ USEUCOM ECSM**

**(a)** Act as the primary focal point for AT/FP for USCINCEUR, and coordinate the establishment of AT/FP responsibilities and procedures for the USDR.

**(b)** Monitor and assist USDR's, within the USEUCOM AOR, with implementation of AT/FP programs.

**(c)** In coordination with ECJ5, and ECJ4 for Turkey, act as interface on AT/FP issues with the USDRs, to streamline the process, by providing them a single point of contact.

**(d)** As required, periodically assist in the conduct of comprehensive, or specifically focused security reviews in situations or locations where a unique threat exists, DoD provides substantial security support, or there is significant command interest.

**(2) HQ USEUCOM ECJ1.** In coordination with the Service component command Personnel Directorates, ensure all PCS and TDY orders for personnel stationed in USEUCOM indicate the requirement for Level I AT/FP training. Also, require theater clearance approvals and TDY orders to specify the authority responsible for security, either USCINCEUR or the appropriate COM, and the local point of contact for AT/FP matters.

**(3) HQ USEUCOM ECJ5.** Act as the HQ USEUCOM Office of Primary Responsibility (OPR) for administering the USDR program. Coordinate all issues involving the USDR and impacting on AT/FP with ECSM.

**(4) U.S. Defense Representative (USDR).** Act as the senior officer responsible for coordination of AT/FP issues for DoD elements under security authority of the COM. Serve as the primary conduit between the CINC and the COM for all AT/FP matters.

**(a)** Function as the single point of contact for AT/FP of all DoD elements and personnel who are the security responsibility of the COM. As such, these elements are under the cognizance of the USDR for AT/FP when the USDR is acting on behalf of the COM. Coordinate all AT/FP matters and issues with the RSO (or the COM's senior

**C-4-2**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

advisor for security matters) and HQ USEUCOM ECSM, as well as appropriate DoD elements and personnel.

**(b)** Coordinate with the RSO to determine if all DoD elements and personnel receive security support comparable to that provided to other members of the Country Team. Report any disparities in AT/FP coverage that cannot be resolved at the local level to HQ USEUCOM ECSM.

**(c)** In coordination with the RSO/PSO, provide advice and information to the COM concerning AT/FP and security of all DoD elements and personnel. Represent USCINCEUR as well as other DoD elements and personnel at country team meetings, such as the Emergency Action Committee (EAC) or other appropriate forums.

**(d)** Act as point of contact for USCINCEUR in developing, coordinating, finalizing, and periodically reviewing the COM-CINC MOA on security. Coordinate these actions with HQ USEUCOM ECSM. Per references (c) and (d), monitor the inventory of all DoD elements and personnel in-country and report changes to HQ USEUCOM ECSM as required.

**(e)** The DoD Terrorist Force Protection Condition system does not apply to DoD elements who are under the security responsibility of the COM. Overseas Security Policy Board (OSPB) standards, as supplemented by the COM, will be followed. These standards may be found in DOS Volume 12 of the Foreign Affairs Manual (FAM 12). The USDR may evaluate DoD Force Protection Condition and AT/FP measures that would be appropriate for implementation and work through the RSO to incorporate these measures when and where prudent.

**(f)** Ensure procedures are established to provide 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.

**(g)** Provide AT/FP inputs related to DoD elements, personnel and activities to the Emergency Action Plan (EAP) for the diplomatic mission. Verify DoD elements and personnel under the cognizance of the USDR have local implementing procedures.

**(h)** Recommend to HQ USEUCOM ECSM any billets requiring resident AT training. Intent is to ensure such billets are properly coded by parent services to require resident AT training prior to assignment.

**(i)** In cases where the USDR is the approval authority for country and/or theater clearances, ensure requests (if required by DoD Foreign Clearance Guide) specify personnel traveling TDY to the country have received required Level I AT/FP training prior to travel and are aware of public announcements or travel warnings in

## FOR OFFICIAL USE ONLY

effect. If the approving authority, disapprove any country/theater clearance requests unless travelers certify that required training has been received. Also, verify that TDY orders specify responsibility (COM or USCINCEUR) for security (AT/FP) and list the local point of contact for AT/FP matters.

**(j)** Determine if newly arrived DoD personnel (PCS) have received Level I AT/FP training as mandated by DoDI 2000.16. If personnel have not received AT/FP training, advise HQ USEUCOM ECSM. Require DoD personnel to attend such security training and orientations as directed by the RSO/PSO or COM.

**(k)** In coordination with the RSO/PSO, verify all DoD elements and personnel under the security authority of the COM are included in security reviews conducted by the RSO.

**(l)** In coordination with the COM and RSO/PSO, assist HQ USEUCOM ECSM with reviews of security support provided to DoD elements and personnel under the security responsibility of the COM.

**(m)** Exercise directive authority for security over all in-country DoD elements and personnel for whom COM has security responsibility in cases of emergency wherein U.S. national or DoD interests are involved and the urgency of the situation precludes referral up the chain of command to USCINCEUR. This shall not preempt the authority exercised over non-CINC assigned elements and personnel by the COM or the mission authority exercised by parent DoD components. Directive authority includes tactical control (TACON) for force protection of all in-country non-CINC assigned DoD elements and personnel assigned or temporarily assigned to the AOR (to include aircraft and their crews). TACON for force protection enables the USDR to order implementation of force protection measures and to exercise the security responsibilities outlined in any COM/CINC MOA for security.

**(n)** Verify with the RSO/PSO that all DOD elements and personnel for whom the COM has security responsibility are receiving security support comparable to that provided to other members of the country team. DODD 2000.12 requires USCINCEUR, in coordination with the COM, to review the AT/FP status of all DOD activities and personnel under the AT/FP responsibility of the COM.

**(1)** These reviews will generally be conducted annually, in coordination with the review of the COM/CINC MOA on security responsibility.

**(2)** The USDR will contact DoD elements as part of the review process to verify security support is being provided and to identify any previously unidentified security issues or concerns.

**(3)** Additionally, the USDR will recommend to HQ USEUCOM ECSM any billets requiring resident AT training. Intent is to ensure billets are properly coded by parent services to require resident AT training prior to assignment.

**C-4-4**

**FOR OFFICIAL USE ONLY**



## FOR OFFICIAL USE ONLY

(4) Should the review identify security issues or concerns, the USDR is encouraged to attempt resolution of these issues with the RSO/PSO or other appropriate embassy staff. The USDR will advise HQ USEUCOM ECSM of any security issues that cannot be resolved locally, or those that require HQ USEUCOM action or assistance.

(5) Results of the security review will be provided to HQ USEUCOM ECSM via message or memorandum.

**(5) All Commands (non-CINC assigned forces) and Defense Agencies** with DoD elements and personnel, for whom the COM has security responsibility, shall ensure those elements and personnel coordinate AT/FP requirements and issues with the USDR.

### c. Coordinating Instructions.

(1) Nothing in this Appendix relieves the unit or element commander of the ultimate responsibility for the protection of his/her unit personnel. Deployed unit and element commanders will use their normal chain of command for reporting AT/FP incidents or issues. All resource, manpower and other requests for AT/FP assistance will be submitted through normal Service channels for execution, with information copies to HQ USEUCOM ECSM for the purpose of monitoring and tracking requirements.

(2) Nothing in this Appendix changes the following command relationships:

(a) The military chain of command, from USCINCEUR to the subordinate commanders of forces assigned or designated as being under the CINC for force protection.

(b) The authority of the Service Chiefs, Military Departments or Defense Agencies to exercise technical, substantive, and policy control; and control over internal administration of their various elements.

(c) The normal direct access of the military attachés and the chiefs of security assistance organizations to host government, military, and other officials.

(d) Command relationships, responsibilities, and functions of the DoD elements as provided in appropriate directives or detract from the USDR's special relationships with appropriate officials.

(e) Relationships and responsibilities between the Military Service attachés and the Chiefs of their Services and Secretaries of their Military Departments.

(f) The Defense Attaché's role as adviser to the COM.

## FOR OFFICIAL USE ONLY

(g) The position of individuals specifically designated as representatives of the Secretary of Defense or Chairman, Joint Chiefs of Staff.

(3) For those matters pertaining to AT/FP responsibilities governing DoD elements and personnel under the COM, the reporting channel for the USDR will be to the COM while keeping USCINCEUR and the parent command/agency informed. For AT/FP matters involving DoD elements under the CINC, the reporting channel will be to USCINCEUR while keeping the COM and the parent command/ agency informed. Reporting channels for all other matters remain unchanged.

(4) When the Defense Attaché is designated the USDR, the attaché title, responsibilities, and reporting channels through DIA are unchanged. However, for the discharge of specific USDR AT/FP responsibilities, the attaché will report to USCINCEUR.

(5) Regardless of cognizance over DoD elements and personnel, the USDR will coordinate any actions impacting on AT/FP and requiring higher headquarters involvement with HQ USEUCOM ECSM and ECJ5. When the USDR is also the Office of Defense Cooperation (ODC) Chief (not the Defense Attaché), ECJ4 will be included in this coordination cycle.

(6) Nothing in this Appendix changes normal reporting channels and direct access to parent organizations/agencies.

(7) Nothing in this Appendix changes various Defense Agency heads' necessary direct access to the COM to fulfill assigned responsibilities and functions.

(8) While executing the AT/FP responsibilities specified in this Appendix, the USDR may not exercise mission-tasking authority over DoD elements and personnel who do not normally report through the USDR in his/her primary duty assignment (unless in cases of emergency as described in paragraph 3b(4)(m), above). The COM will normally exercise AT/FP mission-tasking authority. If there are any problems encountered in this regard, the USDR should report these to HQ USEUCOM ECSM.

(9) The RSO/PSO, and ultimately the COM, are responsible for defining and managing physical security standards for offices and residences for DoD elements and personnel under the COM. This includes both physical security and electronic security safeguards for facilities to include family living quarters. The nature and level of required security enhancements are found in the DOS FAM 12.

(10) To assist the USDR in ensuring adequate security safeguards for residential facilities, the RSO/PSO usually will conduct inspections of quarters prior to occupancy. The monitoring of security and safety safeguards by the RSO/PSO will help ensure minimum residential physical security standards and avert possible oversights in

C-4-6

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

providing safeguards to all homes. If circumstances preclude an actual physical inspection by the RSO/PSO, potential occupants should, at a minimum, obtain a copy of the inspection checklist and complete it prior to accepting new quarters. Leases should not be signed and residences should not be occupied without prior coordination with the RSO/PSO.

**(11) Resolution of a “Conflict on Post” (The term “Post” is a Department of State term which means an overseas diplomatic mission, e.g., embassy or consulate).** A “conflict on post” exists when a disagreement between the USDR and the RSO cannot be resolved by the Emergency Action Committee (EAC) at the mission (commonly referred to as "post") regarding security requirements.

**(a)** Normally a conflict regarding the substance or interpretation of security requirements can be resolved locally between the RSO and the USDR. If resolution is beyond the capability of this level, the matter should be referred to the COM through the EAC for a resolution.

**(b)** If the issue can not be resolved locally and further action is required, the issue will be referred to HQ USEUCOM ECSM.

**(c)** HQ USEUCOM ECSM, ECJ5, and ECJ4 (in cases where the USDR is the ODC Chief, or in cases where the conflict involves the ODC or SAO) will review the dispute and arrive at a course of action to produce resolution. USEUCOM will refer validated disputes with proposed solutions to the DoD Executive Agent (DIA DAC) through the Joint Staff (J34 and J5), with information copies provided USDP-DSCA (for cases involving ODCs or SAOs) and SECSTATE for assistance in resolving the conflict.

**(12)** Military Services, Defense Agencies, and all other DoD activities with individuals in-country must ensure the USDR is informed of the whereabouts of all assigned and/or attached forces and personnel to enable the USDR to fulfill his/her AT/FP responsibilities.

### ACKNOWLEDGE

**JOSEPH W. RALSTON**  
General, USAF

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**C-4-8**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****APPENDIX 5 (AT/FP FORUMS) TO ANNEX C (OPERATIONS) TO USCINCEUR  
AT/FP OPORD 01-01****REFERENCES: See Basic Order**

This Appendix outlines the primary forums within USEUCOM to highlight, explore, track and discuss AT/FP issues at different levels of command.

1. Although not exclusively an AT/FP forum, the Component Commanders Conference (CCC) provides a 4-star oversight forum for the heads of each of the service component commands and USCINCEUR to discuss and review AT/FP issues. The CCC usually meets on a quarterly basis.
2. The General/Flag Officer Antiterrorism Steering Group (GOASG) is the HQ USEUCOM forum, chaired by the Chief of Staff with participation of the service component commands and key members of the USEUCOM senior staff.
3. The USEUCOM Joint Antiterrorism Working Group (JAWG) is the recognized forum for component command AT/FP program managers to coordinate initiatives and resolve issues.
4. The HQ USEUCOM AT/FP Senior Threat Working Group (STWG) or a comparable forum is a senior officer group (O-6 level), led by the senior USEUCOM officer responsible for AT/FP program management, the Special Assistant for Security Matters (SASM). The STWG is the decision-making body responsible for resolving AT/FP issues and approving AT/FP policies based on recommendations from the HQ USEUCOM AT/FP Threat Working Group (TWG). The STWG meets at the discretion of the SASM.
5. The HQ USEUCOM AT/FP TWG is a staff officer level working group chartered to facilitate rapid coordination and resolution of AT/FP issues. The AT/FP TWG provides staff support to the AT/FP STWG and meets at the discretion of the SASM. The TWG normally consists of decision-making representatives from the law enforcement, security, intelligence, and counterintelligence communities as well as other HQ USEUCOM staff elements. The 6 ASG Antiterrorism Officer (ATO) may participate in the TWG when appropriate. The TWG integrates threat information and law enforcement-derived information to make AT/FP force protection recommendations to the AT/FP STWG.

**FOR OFFICIAL USE ONLY**

**ACKNOWLEDGE:**

**JOSEPH W. RALSTON**  
General, USAF

**TABS:**

- A. General/Flag Officer Antiterrorism Steering Group
- B. USEUCOM Joint Antiterrorism Working Group

**C-5-2**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### **TAB A (GENERAL/FLAG OFFICER ANTITERRORISM STEERING GROUP) TO APPENDIX 5 (AT/FP FORUMS) TO ANNEX C (OPERATIONS) TO USCINCEUR AT/FP OPOD 01-01**

**1. GENERAL.** The General/Flag Officer Antiterrorism Steering Group (GOASG) provides senior (Director and Special Staff Principal) oversight for AT/FP issues within the command. The Steering Group is the highest authoritative body responsible to the USCINCEUR and DCINCEUR for addressing AT/FP issues and recommending courses of action for theater-wide AT/FP activities. The Steering Group's composition provides USCINCEUR and DCINCEUR a multi-disciplined forum for ensuring the security, safety, and protection of DoD personnel, family members, and facilities throughout the USEUCOM AOR.

**2. COMPOSITION.** The HQ USEUCOM Chief of Staff chairs the GOASG. The standing membership includes the USEUCOM Staff Directors, USEUCOM Special Staff Principals, and senior Service component command representation.

**3. FREQUENCY OF MEETINGS.** Quarterly, or as requirements dictate.

#### **4. PURPOSE**

**a.** Provide oversight/guidance for the execution of the following AT/FP provisions in the USEUCOM AOR for USCINCEUR and DCINCEUR:

**(1)** Create a level of awareness, appreciation, and readiness commensurate to the threat.

**(2)** Ensure proper coordination of AT/FP policies and measures to protect DoD personnel and their family members, facilities, resources, and equipment throughout the USEUCOM AOR from terrorist acts and to assist subordinate commanders in implementing Military Service programs.

**(3)** Ensure Force Protection Conditions are uniformly implemented as specified in DoD Directive 2000.12.

**(4)** Ensure active coordination with COMs and host nation officials for the protection of DoD personnel serving at U.S. missions in USEUCOM AOR.

**b.** Provide oversight for the execution of USCINCEUR's AT/FP strategy and guidance as articulated in the USEUCOM Force Protection Campaign Plan as part of the Theater Security Planning System (TSPS) and USCINCEUR Policy Letters.

**c.** Conduct reviews of the AT/FP programs and initiatives within the command.

**d.** Approve, prioritize, and track AT/FP funding projects within the command.

**C-5-A-1**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

e. Provide senior level emphasis and support for AT/FP programs, policies, procedures, initiatives, and actions.

f. Provide recommendations on how to deal with terrorist threats in the AOR.

**5. RESPONSIBILITIES.** The following agencies are the lead organizations for the responsibilities listed.

a. **HQ USEUCOM Chief of Staff.** Chair the GOASG meetings and provide appropriate feedback to USCINCEUR and the DCINCEUR on the command's AT/FP initiatives, programs, and postures within the theater.

b. **HQ USEUCOM Staff Directors and Special Staff Principals.** Provide directorate/special staff updates on current DoD, Joint Staff, USEUCOM, Joint Task Force (JTF) and/or Combined Task Force (CTF) AT/FP actions and initiatives in associated functional areas. ECSM will provide a meeting agenda with topics of discussion to the principals prior to each meeting.

c. **Service component commands.** Provide Deputy Commander or General/Flag Officer representation to the GOASG. Provide updates on current component command AT/FP actions and initiatives. Provide prioritized funding projects and budget initiatives for AT/FP requirements.

**d. HQ USEUCOM ECSM**

(1) Act as the proponent for scheduling the Steering Group meetings.

(2) Coordinate with the HQ USEUCOM Secretary of the Joint Staff (SJS) for meeting times and location. Schedule video teleconferences with all of the Service component commands.

(3) Provide all administrative functions for the GOASG to include the publishing of future agendas, topics of discussion, and read-ahead packets.

(4) Record, publish, and distribute the minutes of each GOASG meeting to each of the participants.

(5) Convene the ASAWG to coordinate and facilitate any HQ USEUCOM AT/FP staff actions that may arise from GOASG meetings.



## FOR OFFICIAL USE ONLY

### **TAB B (USEUCOM JOINT ANTITERRORISM WORKING GROUP (JAWG)) TO APPENDIX 5 (AT/FP FORUMS) TO ANNEX C (OPERATIONS) TO USCINCEUR AT/FP OPOD 01-01**

**1. GENERAL.** The USEUCOM JAWG is the recognized forum for information exchange and program interface among representatives from the Service component commands and other security/antiterrorism/intelligence organizations. The JAWG provides a forum for consultation on matters of mutual concern regarding the entire spectrum of terrorism as well as anti-U.S./NATO protest activity.

**2. COMPOSITION.** The JAWG consists of:

- a. Primary proponents for AT/FP from HQ USEUCOM, HQ USAREUR, HQ USNAVEUR, HQ USAFE, HQ MARFOREUR, and HQ SOCEUR.
- b. HQ USEUCOM Special Assistant for Security Matters (ECSM) chairs the forum.
- c. HQ USEUCOM Intelligence Directorate, Operations Division (ECJ23).
- d. Senior U.S. representative from the Provost Marshal, SHAPE.
- e. 2nd Region, U.S. Army Criminal Investigation Command.
- f. Air Force Office of Special Investigations (AFOSI), Region 5.
- g. Naval Investigative Service Regional Office, Europe.
- h. ACE Counterintelligence Activity (650<sup>th</sup> MI Group).
- i. Additional representatives from HQ USEUCOM, the Service component commands, or other agencies may be regular attendees at the call of the membership and approval of the chairman. Permanent members may invite guests to attend meeting subject to coordination with and approval of the JAWG chairperson.

**3. FREQUENCY OF MEETINGS.** Semiannually, or as requirements dictate. Permanent member organizations will alternate as the host for meetings.

**4. PURPOSE.** The charter of the JAWG includes:

- a. The review of current intelligence/information exchange regarding the terrorist threat throughout the USEUCOM AOR.
- b. The discussion of current and proposed AT/FP policy and programs.
- c. The coordination of AT/FP procedural matters among HQ USEUCOM, Service component commands, and theater agencies.

**C-5-B-1**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

**d.** The exchange of developed proactive AT/FP initiatives and programs.

**e.** The discussion and periodic review of the non-tactical armored vehicle (NTAV) program, the Firearms for Personal Protection Program, and High Risk Personnel (HRP) Protective Services program within USEUCOM. This includes HRP Protective Service programs involving the protection of senior U.S. personnel serving in NATO and other international assignments.

**f.** The discussion and periodic review of present and proposed terrorist awareness and AT/FP training programs within USEUCOM to include equipment evaluation.

**g.** The consideration of Service component command planning guidance concerning AT/FP countermeasures and instructions/guidance pertaining to the control of civil disturbances.

**h.** The identification of current or potential AT/FP problem areas and formulation of recommended solutions that may require theater-wide guidance.

### **5. RESPONSIBILITIES. HQ USEUCOM ECSM**

**a.** Acts as the proponent for the USEUCOM JAWG.

**b.** Publish announcements of the USEUCOM JAWG meetings, agenda, and related administrative data.

**c.** Prepare and disseminate the minutes of the USEUCOM JAWG meetings NLT 14 days after the meeting.

**C-5-B-2**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### APPENDIX 6 (CRISIS ACTION RESPONSE) TO ANNEX C (OPERATIONS) TO USCINCEUR AT/FP OPORD 01-01

#### REFERENCES: See Basic Order

**1. GENERAL.** Initial response to a crisis is critical to successful recovery and resumption of the mission. No two incidents are exactly the same, but lessons can be drawn from the past to assist in proper response to a future crisis. This Appendix includes items of concern that were factors in previous incidents. Consider these items for applicability to any incident or crisis situation in the future.

**2. LEAD AGENCY.** DOS is the lead agency for the consequence management of terrorist incidents outside the United States. The initial USG effort will be coordinated through a Foreign Emergency Support Team (FEST) led by DOS with its Consequence Management Response Team (CMRT).

**3. EXECUTION.** Consider the following as possible requirements, and structure planning for execution along these lines. At the HQ USEUCOM level, ECSM, in coordination with ECJ2, ECJ3, and ECSO, will prompt the people on scene to ascertain specific requirements. HQ USEUCOM (ECJ3, ECJ4, ECJ5, and ECSO) will then coordinate with supporting commands/agencies and the COM in the affected county or region to execute approved requirements. Intra-theater support normally will be coordinated by or through Component Commanders in coordination with the HQ USEUCOM European Theater Command Center (ETCC) or Crisis Action Team (CAT). Local commanders and/or the USDR will evaluate and validate on-scene requirements, forwarding to HQ USEUCOM those requiring external assistance/coordination. USCINCEUR CONPLAN 0400-XX (S) provides detailed instructions for consequence management operations.

**a. Initial Notification Requirements - IMMEDIATE ON-SCENE.** Unit/activity chain of command on the scene will ensure the rapid notification of the following:

<input type="checkbox"/> (1) UNIT MEMBERS (particularly if threat remains or is unknown)
<input type="checkbox"/> (2) Other DoD elements (if threat may affect them)
<input type="checkbox"/> (3) USDR who in turn notifies the COM (as applicable)
<input type="checkbox"/> (4) HQ USEUCOM ETCC
<input type="checkbox"/> (5) Parent Command (if applicable)

**b. Initial Notification Requirements - FOLLOW ON.** The USEUCOM ETCC will execute appropriate OPREP-3 and/or other required notifications following consultation with ECJ3. The ETCC will also notify the following personnel/headquarters:

<input type="checkbox"/> (1) CINC, DCINC, ECCS
<input type="checkbox"/> (2) ECJ1, ECJ2, ECJ3, ECSM, ECSO, ECPA, ECMD
<input type="checkbox"/> (3) Other Directorates (as applicable)

## FOR OFFICIAL USE ONLY

- |   |
|---|
| <input type="checkbox"/> (4) NMCC and NMJIC             |
| <input type="checkbox"/> (5) ASD:SO/LIC                 |
| <input type="checkbox"/> (6) Service Component Commands |

**c. Data Collection and Reporting.** Gather as much information as possible for initial notification report, but *do not delay notification to gather complete data*. Submit all OPREP-3 reports as soon as possible after an event or incident has occurred and send at FLASH precedence. The goal is to make initial voice reports to USEUCOM ETCC within 15 minutes of an incident, with message reports submitted within 1 hour of the incident. Use all sources, including host nation agencies, to gather data (who, what, when, where, how). Submit updates as required by USEUCOM ETCC. Initial reports should focus on acquiring the following information:

- |   |
|---|
| <input type="checkbox"/> (1) CASUALTIES (total U.S. military, family members, DoD civilians, other AMCITs, and third country national (TCN)). |
| <input type="checkbox"/> (2) TYPE OF INCIDENT (shooting, bombing, etc.)   |
| <input type="checkbox"/> (3) WEAPONS USED (if applicable)   |
| <input type="checkbox"/> (4) STATUS OF PERPETRATORS.  |
| <input type="checkbox"/> (5) ASSESS VULNERABILITY OF SITE, AS WELL AS REMAINING SITES AND PERSONNEL.  |

**d. Possible Initial Requirements.** Determine initial requirements for support of the following functional support areas. Provide specifics for each requirement where possible (i.e. how much, how many, when do you need it, recommended delivery mode, delivery location, etc.):

- |  |
|--|
| <input type="checkbox"/> (1) MEDICAL SUPPORT (Aeromedical Evacuation Teams, Surgeons, etc.)  |
| <input type="checkbox"/> (2) STRESS MANAGEMENT TEAMS   |
| <input type="checkbox"/> (3) EOD TEAMS   |
| <input type="checkbox"/> (4) AUGMENTATION OF SECURITY FORCES (U.S. or host nation)   |
| <input type="checkbox"/> (5) AUGMENTATION OF SECURITY EQUIPMENT (U.S. or host nation)  |
| <input type="checkbox"/> (6) RESCUE TEAMS/EQUIPMENT  |
| <input type="checkbox"/> (7) SEARCH TEAMS/DOGS   |
| <input type="checkbox"/> (8) COMMUNICATIONS EQUIPMENT AUGMENTATION   |
| <input type="checkbox"/> (9) INTERAGENCY COORDINATION (DOS, FBI, etc.)   |
| <input type="checkbox"/> (10) CASUALTY NOTIFICATION PROCEDURES   |
| <input type="checkbox"/> (11) PUBLIC AFFAIRS RELEASES  |
| <input type="checkbox"/> (12) LEGAL SUPPORT AND REQUIREMENTS   |
| <input type="checkbox"/> (13) TRANSPORTATION OF REMAINS (mode of transportation, escorts, departure/arrival ceremony, family member coordination, etc.). |
| <input type="checkbox"/> (14) PERSONNEL REPLACEMENT  |
| <input type="checkbox"/> (15) SAFE HAVEN PROCEDURES FOR PERSONNEL  |
| <input type="checkbox"/> (16) EVACUATION OF PERSONNEL  |
| <input type="checkbox"/> (17) HOST NATION COORDINATION (increases in security, investigation   |

**C-6-2**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

cooperation, medical support, etc.)

□ (18) TRANSPORTATION COORDINATION ASSISTANCE (inter/intra theater lift coordination to support external support provided, e.g., FBI, U.S. security augmenters, evacuation support, etc.)

**e. ECSM Support.** ECSM personnel (many having a Military Police or Security Forces background) may be able to provide on-the-spot expertise and advice on the full range of security subjects, such as personnel movement control, airfield security, etc.

### ACKNOWLEDGE:

**JOSEPH W. RALSTON**  
General, USAF

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**C-6-4**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****APPENDIX 7 (READINESS REPORTING) TO ANNEX C (OPERATIONS) TO  
USCINCEUR AT/FP OPOD 01-01**

<b>REFERENCES:</b>	a. CJCS Guide 3401A, CJCS Guide to the Chairman's Readiness System, Jul 97
--------------------	--

**1. GENERAL.** USEUCOM conducts a theater-wide review of force protection readiness on a quarterly and annual basis using several inter-linked systems, such as the Joint Monthly Readiness Report (JMRR) and the Joint Warfighting Capabilities Assessment (JWCA). These reporting mechanisms provide means to track and report force protection readiness as well as to raise and address force protection issues with the Joint Staff and the Services.

**2. JMRR.** The JMRR provides an ongoing assessment of USEUCOM's readiness to execute the National Military Strategy (NMS) through a comprehensive, current overview of unit and joint readiness and commitments at all three levels of war: tactical, operational, and strategic. Force protection readiness status of each of the component commands and HQ USEUCOM is reviewed as part of the JMRR. Force protection issues should be highlighted separately in the JMRR, but categorized into one of the eight functional areas in the JMRR. Force protection related issues are assessed and assigned a color-coded indicator to indicate the current force protection readiness of the component command across the theater on a given date. Typically, as a part of the full JMRR process, HQ USEUCOM and the component commands then have to assess force protection readiness in the USEUCOM AOR out to some future date (usually to 1 year) and also on some possible scenario occurring that would impact USEUCOM (e.g., a major theater war). For example, is it expected that force protection readiness will improve or decline over time? What, if any, impact will a Major Theater War (MTW) have on force protection readiness in this theater?

a. The JMRR process rates each functional area using color-coded C-LEVELS.

(1) C-1 (DARK GREEN) = the command/agency has only **minor deficiencies** with negligible impact on capability to perform required missions.

(2) C-2 (LIGHT GREEN) = the command/agency has **some deficiencies** with limited impact on capability to perform required missions.

(3) C-3 (AMBER) = the command/agency has **significant deficiencies** which prevent it from performing **some** portions of required missions.

(4) C-4 (RED) = the command/agency has **major deficiencies** that **preclude** satisfactory mission accomplishment.

b. Component commands should consider using a roll-up of the ratings assigned to their subordinate installations/activities from self-assessments or vulnerability assessments when determining the overall component command AT/FP readiness for the JMRR report. A detailed discussion of the management of information concerning vulnerability assessments is found in Annex M, Appendix 2.

**C-7-1**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**3. JWCA.** In some cases, issues raised in the JMRR process may be included in the JWCA process. The JWCA, under the purview of the Joint Requirements Oversight Council (JROC), includes a systematic analysis of the capabilities and requirements of future forces. Thus current capabilities shortfalls that impact force protection, but for which there is no available system to correct the problem are candidates for inclusion in the JWCA. A force protection issue will be included in one of the eleven long-term assessment areas conducted by the Joint Staff. Results of JWCA analyses and their review by the JROC, submitted through the CJCS, may result in changes to the Defense Planning Guidance or changes in Service POMs.

**ACKNOWLEDGE:**

**JOSEPH W. RALSTON**  
**General, USAF**



# FOR OFFICIAL USE ONLY

## ANNEX D (LOGISTICS) TO USCINCEUR AT/FP OPORD 01-01

**REFERENCES:** See Basic Order

This Annex covers specific AT/FP logistics and resource standards, policies and procedures.

**ACKNOWLEDGE:**

**JOSEPH W. RALSTON**  
General, USAF

### **APPENDICES:**

1. AT/FP Design Standards
2. VTER Management Decision Program (MDEP) Funding
  - TAB A:** Unfinanced Requirement Request Format
3. Combating Terrorism Readiness Initiatives Fund (CbTRIF)
  - TAB A:** CbTRIF Submission Format
  - TAB B:** Quarterly CbTRIF Report Format
  - TAB C:** Monthly Obligations Status Report
4. Combating Terrorism Technology Requests
  - TAB A:** Combating Terrorism Technology Request Format

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**D-2**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**APPENDIX 1 (AT/FP CONSTRUCTION DESIGN STANDARDS) TO ANNEX D (LOGISTICS)  
TO USCINCEUR AT/FP OPOD 01-01**

- REFERENCES:**
- a. DoD 2000.12-H, DoD Antiterrorism Program Policies, Guidance, and Mandatory Standards, Jul 93, with Change 2
  - b. DOD 2000.16, "DOD Combating Terrorism Program Standards, January 8, 2001.
  - c. USACE 800-1, Architectural and Engineering Technical Instructions
  - d. TM 60-A-1-1-4, Explosive Ordnance Disposal Procedures - Protection of Personnel and Property, 24 Sep 90
  - e. TM 5-855-1/AFPAM 32-1147/NAVFAC P-1080/DAHSCWEMAN-97, Design and Analysis of Hardened Structures for Conventional Weapons Effects, Sep 98
  - f. TM 5-853/AFMAN 32-1071, four volume series on Security Engineering, May 94
  - g. DA PAM 385-64, Ammunition and Explosive Safety Standards, undated
  - h. USACE Memorandum CEMRO-ED-ST (415-10f), 6 Mar 97 (NOTAL) (S)
  - i. Interim Department of Defense Antiterrorism/Force Protection Construction Standards, 16 Dec 99
  - j. Mil Handbook 1013/1A, Design Guidelines for Physical Security of Facilities, 28 Jun 93
  - k. Mil Handbook 1013/10, Design Guidelines for Security Fencing, Gates, Barriers and Guard Facilities, 14 May 93
  - l. Mil Handbook 1013/12, Evaluation and Selection Analysis of Security Glazing for Protection Against Ballistic, Bomb, and Forced Entry Tactics, 10 Mar 97
  - m. Mil Handbook 1013/14, Selection and Application of Vehicle Barriers, 1 Feb 99
  - n. USEUCOM Directive 61-4, Construction, Apr 98
  - o. American Society of Civil Engineers Standard (ANSI/ASCE 7-98), Minimum Design Loads for Buildings and Other Structures

**1. SITUATION.** This Appendix describes the minimum Antiterrorism/Force Protection (AT/FP) design and physical security standards (design standards) that must be incorporated into all DoD inhabited structures in the USEUCOM Area of Responsibility.

**D-1-1**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**a.** For new construction and major renovation, the identified standards will be incorporated into the planning, programming, budgeting, and execution of construction activities.

**b.** Component commanders will initiate programs to assess existing structures in accordance with current standards and determine vulnerabilities. While no formal time line is mandated for the completion of upgrades, component commands should prioritize assessment results according to specific risks at each installation. 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.

**c.** 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.

**d.** This appendix constitutes USEUCOM Prescriptive AT/FP Program Standard 28 (other prescriptive AT/FP program standards are contained in Annex M, Appendix 1).

**e.** These standards do not apply to structures used by DoD personnel for whom the US Chief of Mission (COM) has security responsibility. For those facilities, Overseas Security Policy Board Standards apply.

**2. POLICY**

**a.** The desired end-state for the USEUCOM AT/FP Design Standards is a safer environment in which our personnel can live and conduct their operational mission(s). While these standards will not prevent a terrorist attack, their implementation will reduce the opportunity for such an attack and mitigate the effects of an attack on DoD personnel.

**b.** Component commands and Defense Agencies in the USEUCOM AOR will incorporate these design standards to minimize the risk to personnel from terrorist attack.

**c.** HQ USEUCOM sets the minimum design standards and recommended practices. Component commands and Defense Agencies are responsible for ensuring these standards are implemented and that subordinate installation commanders certify that force protection considerations have been incorporated into the project programming/design/construction process (DD Form 1391, design approval, etc.). Installation commanders also 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 TM 5-853/AFMAN 32-1071.

**d.** Although specific minimum standards are provided, inhabited structures shall be designed or modified to achieve a low level of protection against the blast loads from mortars,

**FOR OFFICIAL USE ONLY**

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. The intent is for the structure to survive well enough to allow people inside the building to safely evacuate in the event of an attack, to provide sufficient protection for personnel survivability, and to mitigate collateral damage, without a bunker mentality. After an explosive event, the building may no longer be usable and repair may not be economical.

e. At a minimum, one planning/design engineer from each major area (i.e., ASG, BSB, Air Force Base, NAVSTA, NAS) will be trained in "Security Engineering." Both the U.S. Army Corps of Engineers (USACE), Omaha District, Protective Design Center (CENWO-ED-S) and the Naval Facilities Engineering Service Center (NFESC) offer a course of instruction which fulfills this requirement.

**3. STANDARDS.** AT/FP design standards apply to all locations controlled or used by U.S. military forces and Defense Agencies in the USEUCOM AOR regardless of the current area threat level. The primary purpose of these standards is to protect personnel. Refer to the definitions in paragraph 4d, below, for guidance and clarification of terminology.

a. **Baseline Threat Weapons.** The development of the specific standards considered the following weapons:

(1) **Improvised Explosive Devices (IED).** An explosive device with a net explosive weight of 100 kilograms of TNT equivalent.

(2) **Direct Fire Weapons.** A rocket propelled grenade (RPG-7) with a 500 meter effective range and 568 grams (1.25 lbs) of TNT equivalent shaped charge warhead.

(3) **Indirect Fire Weapons.** The primary threat is assumed to be from 60 mm and/or 82 mm mortars. 60 mm mortar rounds typically contain approximately 200 grams of TNT. The minimum range for most systems is approximately 90 meters with a maximum range of up to approximately 3000 meters. Most 82 mm mortar systems have a minimum range of approximately 90 meters and a maximum effective range of approximately 4300 meters. An 82 mm mortar high explosive rounds' characteristics are varied, with total projectile weights of approximately 3 kilograms and an explosive weight of approximately 1 kilogram of TNT.

(4) **Chemical, Biological, Radiological (CBR) Agents.** At this time it is not possible to quantify a baseline; however, use of chemical agents is viewed as the most likely type of CBR attack to expect.

b. **Required Minimum AT/FP Design and Physical Security Standards.** The following standards shall be applied in accordance with Table D-1-1, Facility Construction Standards Matrix.

**FOR OFFICIAL USE ONLY**

**(1) Screening From Direct Fire Weapons.** Screening shall be installed where observation from off installation is possible. The purpose of screening is not to defeat the projectiles from direct fire weapons, but to prevent targeting of personnel from off the installation. Aluminum louvers, reflective film, or trees are examples of suitable screening. A combination of screening elements may be used with the intent to adequately screen occupants on all stories from targeting by direct fire weapons.

**(2) Building Separation.** When the separation distance between inhabited buildings is less than 10 meters (15 meters for troop billeting / primary gathering spaces), ensure that the building cladding can provide a low level of protection against the design blast pressure from 1-kilogram TNT indirect fire projectile at one-half the available separation distance.

**(3) Perimeter Standoff.** The minimum standoff distance required is 45 meters from the installation, site or facility perimeter. This perimeter may or may not be physically secured (i.e., fence, wall, etc.) but should be defined as the area where control and/or jurisdiction by U.S. forces begins. For facilities less than 45 meters from a perimeter, incorporate hardening of the facility to provide a low level of protection from a 100 kilogram TNT equivalent IED. Never site a facility less than 15 meters from the perimeter. Wherever possible, increase the perimeter standoff. The intent is to prevent mass casualties associated with both building collapse and glass fragmentation hazards.

**(4) Superstructure.** For all structures of three stories or more, design to sustain local damage with the structural system as a whole remaining stable and not being damaged to an extent disproportionate to the original local damage. To achieve this, structural elements must be arranged to provide stability to the entire structural system by transferring loads from any locally damaged region to adjacent regions capable of resisting those loads without collapse. This shall be accomplished by providing sufficient continuity, redundancy, energy dissipating capacity (ductility) or a combination thereof, in the members of the structure. That design analysis will include removal of one primary vertical or one primary lateral load-carrying element without progressive collapse in the event of a close proximity explosion by the design IED. For further guidance, refer to American Society of Civil Engineers Standard 7-98, Minimum Design Loads for Buildings and Other Structures. Only professionally qualified structural engineers, should undertake design and assessment of this standard.

**(5) Window Treatments**

**(a) New Construction or Major Renovation.** Windows must be able to resist blast pressures from an IED with an explosive equivalent of 100 kilograms of TNT at the required/available standoff without creating a high level glass fragmentation hazard to personnel inside the facility. For new construction or major renovation windows shall use, as a minimum, 7.5 mm laminated glass with a minimum interlayer thickness of 1.5 mm. If a double-paned window is installed, the interior pane shall be laminated (7.5 mm minimum). Window frames for these types of glazing constructions must be designed and verified by inspection to ensure proper frame strength and anchorage.

**FOR OFFICIAL USE ONLY**

**(b) Whole Building Window Replacement in Existing Facilities.** Whole facility window replacement shall be undertaken with glazing that is able to resist blast pressures from an IED with an explosive equivalent of 100 kilograms of TNT at the required/available standoff without creating a high level glass fragmentation hazard to personnel inside the facility. As a minimum, 7.5 mm laminated glass with a minimum interlayer thickness of 1.5 mm. If a double-paned window is installed, the interior pane shall be laminated (7.5 mm minimum). Window frames for these types of glazing constructions must be designed and verified by inspection to ensure proper frame strength and anchorage.

**(c) Hazard Mitigation in Existing Buildings: Evaluation Criteria.** All inhabited facilities which do not provide a low glass fragmentation hazard level of protection must be identified in accordance with the administrative reporting requirements of this document. In these facilities later selected for hazard mitigation, window replacement is the preferred method of improvement due to the recurring maintenance and operational requirements **(curtains must be closed, catcher bars must remain in place)** associated with other methods. However, the addition of devices such as fragment retention film (FRF), FRF in conjunction with catcher bars or blast curtains, may be used as appropriate. In cases where glazing will be retrofitted to fracture but remain in the frame, design engineers must evaluate the strength of the window frame and window frame anchorage. In addition, design engineers must determine the proper thickness of film coupled with the best use of catcher bars/blast curtains. Glass replacement with 7.5 mm laminated glass (minimum) is acceptable if frames and anchorage have sufficient strength to transfer the reactions from the glass. If some form of FRF is used in a retrofit application, then a minimum of 4-mil (0.004") or 0.1 mm thick film is required (and must be installed on the inside-facing portion of the glass). Where film is applied such that it extends only to the exposed edges of the glass (daylight application), the energy of the failed glass pane must be sufficiently reduced so that glass fragments are not higher than ½ meter above the floor at a distance of 3 meters into the room. Methods to reduce this effect include adding structural/silicon type caulking to the edges (connecting the film to the window frame), and/or installation of catcher bars or blast curtains.

**(d)** The glazing requirements and criteria outlined in paragraphs (5)(a)-(c), above, need not be applied for windows/openings into typically unoccupied areas, e.g., basements, attics, etc.

**(6) Protection of Entrances and Exits (to include emergency exits).** Locate exterior doors to buildings so they cannot be targeted from vantage points located off the installation. The intent is to prevent personnel evacuating a building from being targeted from off the installation. Exterior doors to inhabited structures will open outward. As a minimum, doors shall be 18 gauge hollow metal and any glazing will be 7.5 mm laminated glass. Intent is to prevent secondary fragmentation hazards.

**(7) Parking Lots and Roadways.** Locate parking lots a minimum of 25 meters and roadways a minimum of 10 meters from inhabited structures. For troop billeting / primary gathering spaces, maintain a minimum standoff distance of 25 meters from roadways. Designated parking for family housing, within secured perimeters with access control, is

**FOR OFFICIAL USE ONLY**

excluded from the 25 meter standoff requirement. However, where standoff distances exist for housing areas, those distances will not be encroached during renovations or upgrades. Parking beneath inhabited buildings is not allowed. Drive up/drop off areas closer than 25 meters are allowed, but facilities with these areas must be designed/modified as follows:

(a) Establish a drive-up and drop off area, or a drive thru lane of traffic, near the building using physical barriers that clearly define the area and the intended use. Physical barriers may include curbing, planters, jersey barriers, etc., or combinations of different systems.

(b) The drop off area shall have signs that clearly identify the location and the intended use. Signs should include wording such as "Do Not Leave Vehicles Unattended", "No Trucks Allowed", "Passenger Loading and Unloading Only", or combinations thereof.

(c) The drive-up or drive-thru area shall be configured such that access to vehicles can be curtailed at Force Protection Conditions that restrict standoff distances.

(d) Access to a drive-up or drive-thru area shall be from a point outside of the standoff zone established for the building. The initial approach shall be parallel to the building or a barrier erected that precludes direct movement towards the building.

**(8) Building Perimeter Protection/Standoff Zone Delineation.** Standoff zones shall have boundaries clearly defined by barriers.

(a) If threat analysis does not identify a moving vehicle bomb tactic, these barriers need not provide physical resistance to stop vehicles. They need 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. "Hard" landscaping, incorporating steps and mounds, is one way to define and maintain standoff. Similarly, the planting of trees or hedges ("soft" landscaping) at strategic points can prevent overlooking and can also be used to define and maintain standoff. However, weigh the employment of such measures against the opportunities that could be presented to an intruder for concealment and/or for the hiding of explosive devices.

(b) When the threat analysis indicates the existence of a moving vehicle threat to a building, concrete bollards or other crash rated vehicle barriers must be considered. The purpose of these barriers are to prevent a vehicle from jumping a curb and parking next to a building or approaching the front entrance. These barriers must be designed based on the expected maximum speed the vehicle can attain based on the site conditions.

**(9) External Storage Areas.** External storage areas shall be sited/relocated as follows:

(a) Troop Billeting/Primary Gathering – 25 meters



**FOR OFFICIAL USE ONLY**

- (b) Inhabited Facilities – 10 meters
- (c) Family Housing (containing more than 12 units) – 25 meters
- (d) Stand Alone Retail facilities and Franchised Operations – 25 meters

The aim is to minimize the effects of a hand placed 23 kilogram IED should one be concealed within these areas. Examples of storage areas include trash containers, recycling bins, stand alone storage buildings, etc.

**(10) Security Lighting.** Incorporate security lighting into the project at the initial planning stage. Requirements for boundary, Entry Control Point, and area lighting must conform to TM 5-811-I/AFM 88-9, based upon the identified facility threat. Lighting for Closed Circuit Television (CCTV), where it is determined to be necessary by other requirements, must be designed in conjunction with the CCTV system in accordance with TM 5-853-4.

**(11) Mail Rooms and Delivery points.** Locate mailrooms and delivery points to the perimeter of inhabited structures. Locate key utilities (including communications, fire detection and alarm, water mains, etc.) and sensitive equipment away from walls common with these areas in inhabited structures. Locate mailrooms and delivery points away from population concentrations. Allow space for security screening devices such as bomb detection equipment.

**(12) Mechanical and Utility Systems.** Locate air intakes at least three (3) meters above existing grade or on the roof of single-story inhabited structures, and restrict access to the intakes. Control access to roofs of inhabited structures. Avoid external ladder access by providing entry from internal stairways or ladders such as in mechanical rooms. Include an emergency shutoff switch in the control system that immediately shuts down the heating, ventilation and air conditioning (HVAC) system of inhabited structures. Ensure that redundant utilities in inhabited structures do not run in the same locations or chases. Secure exterior access to power / heating plants, gas mains, water supplies, communications, electrical service or other support facilities or infrastructure. Construct fire protection systems in inhabited structures using seismic detailing.

**(13) Construction of Temporary / Expeditionary Structures.** Although not specifically required, the design guidance listed above in paragraphs 3b(1) through 3b(12) should be considered when constructing temporary and expeditionary structures. Commanders also are expected to use expeditionary protective measures commensurate with the identified Terrorism Threat Level and existing Force Protection Condition. Examples of expeditionary measures available to reduce primary blast effects and fragmentation are soil berms, sandbags, sand grids, and concrete modular revetments. These and other expeditionary measures are discussed in TM 5-855-1/AFPAM 32-1147/NAVFAC-P-1080/DAHSCWEMAN-97.

**FOR OFFICIAL USE ONLY**

**c. Facility Construction Standards Matrix.** This matrix shows those standards that directly affect DoD owned and leased facilities and must be incorporated. Numbers referenced refer to paragraph 3b, above.

**Table D-1-1, Facility Construction Standards Matrix**

	<b>Troop Billeting</b>	<b>Primary Gathering</b>	<b>Family Housing<sup>1</sup></b>	<b>Inhabited Facilities</b>	<b>Stand Alone Retail &amp; Franchised Operations</b>
<b>Existing Facilities</b>	1, 5-7, 9-12	1, 5-7, 9-12	5-7, 9-12	5-7, 9-12	5-6, 9-12
<b>Major Renovations</b>	1-7, 9-12	1-7, 9-12	2-3, 5-7, 9-12	2-3, 5-7, 9-12	2-3, 5-6, 9-12
<b>New Construction</b>	1-12	1-12	2-12	2-3, 5-12	2-3, 5-6, 9-12
<b>Expeditionary &amp; Temporary Construction</b>	13	13	13	13	13

<sup>1</sup> – Applies only to structures containing more than 12 units.

**d. Additional Design Considerations / Compensatory Measures.** Although not specifically required, the following measures listed below should be considered for incorporation in the design and construction of inhabited facilities.

**(1) Perimeter Counter-mobility.** All installations 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)** 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)** Where a moving vehicle threat is identified through threat analysis, 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 shall be considered when selecting crash rated perimeter barriers. Calculate requirements by using procedures in TM 5-853/AFMAN 32-1071 and Mil Handbook 1013/1A.

**(2) Perimeter Security and Control of Entry to Installation.** Consider protecting the installation by a perimeter security fence through which access is controlled at an established entry control point. Effective security lighting at the entry points to support the security check and inspections should be incorporated at the design stage.

**FOR OFFICIAL USE ONLY**

(a) The entry control point must be able to process vehicles in such a way that during increased Force Protection Conditions entry is not impeded, thus impairing traffic flow. The reason for this is twofold: (a) to prevent personnel awaiting entry from becoming vulnerable to attack; and (b) to prevent pressure being put on the guards to forgo security checks in order to speed up traffic flow.

(b) 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.

(c) Where indicated by threat analysis, provide shielding or hardening of the guard structure to protect entry control point guards against drive-by attacks using small arms. The entry 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.

**(3) Access Roads.** Consider siting the main headquarters building and areas 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 to standoff attack.

**(4) 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:

(a) Away from windows, external doors and external walls.

(b) Toward the center of the building.

(c) Generally not in stairwells or areas having access to an elevator shaft since blast overpressures are likely to propagate into these areas.

(d) Locate in areas surrounded by full height masonry or concrete walls if possible, e.g., internal corridors, internal toilet areas, etc.

(e) 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.

**(5) Location of High-Risk Personnel (HRP) Offices.** Consider locating HRP offices away from over-looking points. These offices should not be sited in areas that would make the

**FOR OFFICIAL USE ONLY**

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.

**(6) 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.

**(7) 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.

**4. ADMINISTRATION**

**a. Reporting Requirements.** All existing inhabited structures will be evaluated against the USEUCOM construction standards contained in paragraph 3b above. Each installation/activity commander will submit through their component command headquarters to HQ USEUCOM ECSM/ECJ4-EN their plan to evaluate existing inhabited structures (including family housing containing more than 12 units). Each installation/activity will also submit through their component command headquarters, a recurring status report to HQ USEUCOM ECSM/ECJ4-EN that delineates the progress made, 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 15<sup>th</sup> of April.

**b. Deviation Program.** The HQ USEUCOM Chief of Staff is the approval authority for any exception, waiver, or variance to the AT/FP construction design standards contained in this OPOD. When circumstances preclude compliance with these standards, installation commanders should submit a request for deviation (exception, waiver or variance) through their component command headquarters to HQ USEUCOM using the format provided at Tab A to this Appendix. Waivers will be considered if compliance with the standard at a particular installation or facility will adversely affect mission accomplishment, unacceptably affect relations with the host nation, exceed local capabilities, or require substantial expenditure of funds at a location where forces will be removed or relocated in the near future.

**(1) Types of Deviations.** All requests for deviations from AT/FP design standards will be identified in one of the following three categories:

**(a) Permanent Deviations (Exceptions).** Permanent deviations, or Exceptions, must be requested when a condition of non-compliance exists that cannot be corrected, or

**FOR OFFICIAL USE ONLY**

when compliance would result in more serious vulnerabilities/problems, or not produce a cost effective solution. Permanent deviations require compensatory measures and have no expiration dates.

**(b) Temporary Deviations (Waivers).** Temporary deviations, or Waivers, must be requested when a correctable, condition of non-compliance exists and can not be immediately corrected. All requests for Waiver will identify compensatory measures and specify an anticipated date for correcting the condition of non-compliance. Waivers will not be approved for more than one (1) year for Significant and High Terrorism Threat Level areas, and not more than two (2) years for all other locations. Subsequent requests for the extension of waived requirements will be considered for approval when fully justified.

**(c) Technical Deviations (Variances).** Technical deviations, or Variances, should be requested when a condition exists that satisfies the intent of the requirement and does not threaten security, but technically differs from specifications directed by higher headquarters. Conditions approved as Variances may or may not require compensatory measures or further actions.

**(2)** Using the format in Tab A to this Appendix, ensure that all deviation requests specify the category (Exception, Waiver or Variance), and as a minimum, include the following:

**(a)** Identify the particular standards for which an exception, waiver, or variance is requested.

**(b)** Describe the full scope of the deviation requested and the expiration date.

**(c)** Describe the anticipated impact of the deviation, if any, on the safety of DoD elements and personnel.

**(d)** Describe the justification for the deviation, and if an Exception (permanent deviation) is being requested, explain why a partial and/or temporary deviation would not be sufficient.

**(e)** Where applicable, describe attempts to comply with standards that have not been approved by host nation officials.

**(f)** Provide an engineering analysis to support the use of mitigating measures in lieu of strict compliance with the stated standard, its cost, and estimated completion date.

**c. Points of Contact.** The following points of contact and references may prove useful when applying the guidance in this Appendix.

**(1)** Joint Staff (J-34), Combating Terrorism Division, is the single point of contact and coordinator for AT/FP matters on the Joint Staff.

**D-1-11**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

(2) United States Army Corps of Engineers Europe District is a construction agent for the design and construction execution of facilities in the USEUCOM 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) Atlantic Division, Naval Facilities Engineering Command (LANTDIV). LANTDIV is a construction agent responsible for design and construction execution of facilities in the USEUCOM AOR. As such, they coordinate blast engineering with the Naval Facilities Engineering Service Center in Port Hueneme, California.

(4) HQ USAFE/CEW is a construction agent responsible for design and construction execution of facilities in the USEUCOM 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) Defense Threat Reduction Agency (DTRA). DTRA is the lead agency for conducting Joint Staff sponsored blast testing and vulnerability assessments.

(6) *Staatsbauamt* is a construction agent responsible for design of facilities in Germany.

(7) Design and execution of minor construction and O&M funded repair work are typically accomplished by the Service component 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.

**d. Definitions.** The following definitions of Engineering related terms are provided as a ready reference. For additional definitions, see the Glossary in Annex Y of this OPORD.

(1) **Billeting.** Any building in which five (5) or more unaccompanied DoD personnel are routinely housed. For the purposes of this document, billeting also will include temporary lodging facilities.

(2) **Catcher-bar.** Typically a metal bar that spans across the inside of the window horizontally at mid-height of the glazing and is fastened to the wall on either side of the window. This bar catches laminated glass as it exits its frame under blast loading.

(3) **DoD personnel.** For the purpose of this Appendix, any U.S. military, DoD civilian, or their family members.

(4) **Expeditionary structures.** Structures intended for use for a period of less than one year. Expeditionary structures are normally lightweight, re-locatable and constructed using war reserve materials such as Harvest Falcon, Force Provider, and Clamshell systems.

(5) **Facility.** Any single building, project, or site.

**FOR OFFICIAL USE ONLY**

**(6) Fragmentation Retention Film (FRF).** A thin optically clear film applied to glass to minimize the spread of glass fragments when the glass is shattered. The film may also be treated with reflective coatings to provide obscuration.

**(7) Military Family Housing (or Family Housing).** An inhabited structure specifically identified as DoD Family Housing that contains more than 12 units. This category specifically does not include unaccompanied dormitories/barracks (see **Billeting.**)

**(8) Inhabited structure.** Structures or portions of structures intended to be occupied by DoD personnel with a density of greater than one person per 40 square meters. This density generally excludes industrial and storage facilities. This does not include buildings with fewer than 5 occupants, single and duplex detached family housing, stand alone franchised food operations, and shoppettes. It may include portions of structures in which not all areas have such population densities.

**(9) Glass fragmentation hazard levels.**

**(a) Low hazard level.** Glazing fragments are thrown for a distance of approximately 1-3 meters, but do not exceed a height of 0.5 meters above the floor at the 3 meter distance. Injuries would be limited to lower body cuts, and fatalities would not be expected although there would be some risk to persons within 1-2 meters of the window.

**(b) High hazard level.** Glazing fragments are thrown much further into the room and at a high velocity above the 0.5meter height at the 3 meter range. Serious injuries, including cuts to the upper body and face from the flying fragments would be expected. Fatalities could occur.

**(10) Laminated glass.** Two or more individual sheets of glass bonded together by a polyvinyl butyral (PVB) plastic, or other equivalent material, interlayer.

**(11) Level of Protection.** The degree to which an asset is protected against a tactic based on the asset's value. Levels of protection refer to the amount of damage a structure is allowed to sustain or the probability that an aggressor attack will be defeated by the protective system.

**(12) Low level of protection.** Damaged, Unrepairable. The facility or protected space will sustain a high degree of damage without collapse. Although collapse is prevented, occupants may be injured and other assets may be damaged but will survive. Damaged building components, including structural members, will require replacement. Depending on the scale of the blast damage, its location, and facility characteristics, the facility may be completely unrepairable, requiring demolition and replacement. The damage allowed may make surviving assets vulnerable to subsequent attack.

**FOR OFFICIAL USE ONLY**

**(13) Major renovation.** Modifications to buildings that cost in excess of 50 percent of the replacement cost of the building.

**(14) Primary gathering facility.** A subset of inhabited structures in which 50 or more DoD personnel routinely gather (e.g., office buildings, indoor recreation facilities, schools, AAFES PX/NEX facilities and DoD family housing buildings with more than 12 units).

**(15) Secured perimeter.** An area that is protected by a fence, wall, vehicle barrier, or impassable landform and includes one or more entry control points.

**(16) Stand-alone retail establishment and franchised operations.** Any stand-alone retail establishment, not operated by a DoD Agency. (AAFES/NEX shoppettes and gas stations shall be included in this category).

**(17) Temporary structures.** Structures constructed, purchased, or leased and intended for use for a period of 3 years or less, and are not expeditionary. These structures are often capable of being relocated such as some pre-engineered buildings, trailers, and stress tension shelters.

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
**General, USAF**

**TAB:**

A. Sample Request for Deviation



## **FOR OFFICIAL USE ONLY**

### **TAB A (SAMPLE REQUEST FOR DEVIATION) TO APPENDIX 1 (AT/FP CONSTRUCTION DESIGN STANDARDS) TO ANNEX D (LOGISTICS) TO USCINCEUR AT/FP OPOD 01-01**

1. HQ USEUCOM is the approval authority for all deviations from USCINCEUR directed Antiterrorism/Force Protection (AT/FP) requirements to include AT/FP Design Standards contained in Annex D, Appendix 1. HQ USEUCOM cannot approve deviations from DoD AT/FP requirements to include DoD construction standards. Such deviation requests must be submitted through HQ USEUCOM to the Joint Staff for consideration and action.
2. A deviation request is not required for stand-off requirements, if equivalent protection (hardening of the structure) is provided. In other words, if the required stand-off distance can not be obtained, but the structure is hardened to provide an equal level of protection against a baseline weapon, then no deviation has occurred.
3. The information areas on the sample deviation request form should, when properly filled out, provide approval authorities with sufficient details to reach a decision.
4. Instructions for completing selected items:
  - Item 4: Include information on each deviation if multiple deviation approvals are required. (NOTE: Submit one request for each facility, building, or unique set of circumstances.)

**FOR OFFICIAL USE ONLY**

**CLASSIFICATION**

(FOR CLASSIFICATION GUIDANCE, SEE Annex L to this OPORD 01-01)

**SAMPLE REQUEST FOR USCINCEUR OPORD 01-01 DEVIATION**

FROM: Originating Unit/Agency

THRU:

TO:

HQ USEUCOM / ECSM      or      Component Command HQs (USAREUR / USNAVEUR / USAFE)  
UNIT 30400 BOX 1000  
APO AE 09128

1. TYPE OF REQUEST

- CONSTRUCTION STANDARD / STAND-OFF                       PROCEDURAL  
 THREATCON MEASURE(S)     OTHER

2. TYPE DEVIATION

- EXCEPTION                                       TEMPORARY DEVIATION                       TECHNICAL DEVIATION  
(Permanent)                                      (Waiver)    (Variance)

ITEM 3 - AFFECTED BUILDING, INSTALLATION OR ORGANIZATION / UNIT (Include 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 & 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 =

**CLASSIFICATION**

**FOR OFFICIAL USE ONLY**

**CLASSIFICATION**

ITEM 6 – IF DEVIATION IS REQUESTED FROM A CONSTRUCTION STANDARD OR STANDOFF REQUIREMENT, PROVIDE COST OF:  
A. PLANNED DESIGN /RENOVATION  
B. DESIGNED MODIFICATION TO SUSTAIN STRUCTURAL INTEGRITY FROM EQUIVALENT OF 50 POUNDS TNT EXPLOSIVE PLACED AT 80 FEET AND PERCENTAGE INCREASE FROM 6.A.  
C. DESIGNED MODIFICATION TO SUSTAIN STRUCTURAL INTEGRITY FROM A BASELINE EXPLOSIVE CHARGE PLACED AT 25 METERS AND PERCENTAGE INCREASE FROM 6.A. SEE ANNEX D, APPENDIX 1 FOR THREAT BASELINE WEAPONS AND EXPLOSIVE CHARGES.

IF EXACT COSTS CANNOT BE DETERMINED, REFER TO ARMY TM 5-853-1 / AFMAN 32-1071 (SECURITY ENGINEERING PROJECT DEVELOPMENT) FOR ESTIMATE TABLES.

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.

**CLASSIFICATION**

**FOR OFFICIAL USE ONLY**

**CLASSIFICATION**

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 NOT BEEN APPROVED. PROVIDE SUMMARY OF REQUEST AND RESPONSE.

14.

ITEM 15 – IMPACT STATEMENT (WHAT IS THE IMPACT ON THE ORGANIZATION OR MISSION IF THE 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

**CLASSIFICATION**

**D-1-A-4  
FOR OFFICIAL USE ONLY**



**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**D-1-A-6  
FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****APPENDIX 2 (AT/FP FUNDING) TO ANNEX D (LOGISTICS) TO USCINCEUR AT/FP OPOD 01-01****REFERENCES: See Basic Order**

**1. GENERAL.** AT/FP funding is available to HQ USEUCOM through the Army's VTER Management Decision Program (MDEP). Department of the Army provides HQ USEUCOM with VTER funds. VTER funds are primarily Operations and Maintenance (O&M) appropriations with O&M restrictions. Funds are provided in order for USCINCEUR to meet its force protection responsibilities as outlined in references (g) and (j). VTER funds enable HQ USEUCOM to conduct command vulnerability assessments in an AOR covering 91 countries; provide for physical security upgrades; procure force protection training and guard contracts for direct reporting units (DRU) such as Offices of Defense Cooperation (ODC) and Military Liaison Team (MLT) facilities and personnel; execute vital security site improvements; procure/replace critical security equipment; and permit the Protective Services Detachment serving the USEUCOM staff to conduct advance security missions and training.

**2. MANAGEMENT.** DAMO-ODL centrally manages VTER funds for HQ DA. At HQ USEUCOM, ECSM manages the VTER Funds with ECCM guidance and assistance. VTER funds are budgeted for HQ USEUCOM ECSM, ECSM-PSD, ECJ4-ID, and ECJ5-J security requirements. Funds are normally limited to those aforementioned staff sections; however, other staff sections or direct reporting activities having a valid and urgent AT/FP requirement are advised to submit an unfinanced requirement (UFR) request.

**3. SUBMISSION REQUIREMENTS.** Those HQ USEUCOM staff elements wishing to receive VTER dollars for their AT/FP requirements should submit an unfinanced requirement request, using the format at Tab A of this Appendix, to ECSM for review and submission to the VTER Program Budget Activity Committee (PBAC) that meets on a quarterly to semi-annual basis.

**4. CRITERIA.** Congressional reporting requirements for AT/FP funds mandate use of below listed funding categories. Requesters having AT/FP UFRs should screen requirements against this list to eliminate ineligible projects from consideration before submitting the UFR to ECSM for funding consideration at the VTER PBAC.

**a. Physical security equipment.** Category includes funding for barriers, blast mitigation devices, security communications systems, explosive detection devices, intrusion detection system devices, personnel protection equipment, and other security equipment and sensors.

**b. Physical security site improvement.** Fund use examples include O&M funded minor construction such as perimeter fencing and barriers.

**FOR OFFICIAL USE ONLY**

**c. Physical security management and planning.** Fund use examples include conducting vulnerability assessments for Joint Staff Integrated Vulnerability Assessments (JSIVA), for security reviews of component headquarters, MLTs, and special assessments. Category also covers security training and attendance at AT/FP conferences.

**ACKNOWLEDGE:**

**JOSEPH W. RALSTON**  
**General, USAF**

**TAB:**

A. Unfinanced Requirement Request Format



FOR OFFICIAL USE ONLY

TAB A (UNFINANCED REQUIREMENT REQUEST FORMAT) TO APPENDIX 2  
(AT/FP FUNDING) TO ANNEX D (LOGISTICS) TO USCINCEUR AT/FP OPOD 01-01

HQ U.S. EUROPEAN COMMAND  
FY \_\_ UNFINANCED REQUIREMENT (UFR)

TITLE: \_\_\_\_\_

MDEP: \_\_\_\_\_ PROGRAM ELEMENT: \_\_\_\_\_

SUB-ACTIVITY GROUP (SAG): \_\_\_\_\_ PROGRAM DIRECTOR SAG PRIORITY \_\_\_\_

AMOUNT: \_\_\_\_\_ CAN UFR BE INCREMENTALLY FUNDED \_\_\_\_\_

DROP DEAD DATE FOR FUNDING DURING THE EXECUTION YEAR: \_\_\_\_\_

DESCRIPTION OF REQUIREMENT: \_\_\_\_\_

\_\_\_\_\_

DOES REQUIREMENT ADDRESS AN IDENTIFIED VULNERABILITY \_\_\_\_\_

VAMP/JVAT PROJECT NUMBER: \_\_\_\_\_

IMPACT IF NOT FUNDED (Be specific. Include not only mission impact, but what will NOT  
be funded if resources must be reallocated): \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

PROPONENT POC: \_\_\_\_\_ RM POC: \_\_\_\_\_

APPROVED BY: \_\_\_\_\_ DATE: \_\_\_\_\_

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**D-2-A-2**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****APPENDIX 3 (COMBATING TERRORISM READINESS INITIATIVES FUND) TO ANNEX D (LOGISTICS) TO USCINCEUR AT/FP OPORD 01-01**

<b>REFERENCES:</b>	CJCSI 5261.01A, Combating Terrorism Readiness Initiatives Fund, 1 Aug 98
--------------------	--

**1. SITUATION.** Because of the dynamics of the terrorist threat and evolving mission requirements, new Antiterrorism/Force Protection (AT/FP) requirements may emerge, which require immediate funding to ensure the safety and security of DoD elements and personnel.

**2. MISSION.** To provide a mechanism to fund emergency or other unforeseen high priority Combating Terrorism requirements.

**3. EXECUTION**

**a. Scheme of support.** This appendix establishes policy and procedures to facilitate execution of the Combating Terrorism Readiness Initiatives Fund (CbTRIF) established by the Secretary of Defense and managed by the CJCS. This funding mechanism provides a means for USEUCOM to react to unanticipated requirements stemming from changes in terrorist threat or AT/FP doctrine/standards.

**b. Tasks and Responsibilities****(1) Service component commands**

**(a)** Staff and submit requests in compliance with program guidelines. Submit a courtesy copy of the request to the parent Service. Submit packages to HQ USEUCOM ECSM for review at anytime during the year. Component commands should submit emergency requests as soon as the requirement is identified, and ECSM will coordinate the requests immediately upon receipt. Component commands must submit emergent requests to ECSM NLT 1 October for the December allocation, and 1 February for the April allocation.

**(b)** Expedite obligation of funds received for approved CbTRIF requests. Make every effort to obligate funds as soon as possible after they are received from the Joint Staff.

**(c)** Return funds to the Joint Staff that are determined to be in excess of requirements as soon as possible.

**(d)** Submit quarterly reports to HQ USEUCOM ECSM during the execution of the funded project(s) for the first three quarters of the FY. In the last quarter of the FY, submit a monthly report. The report is due NLT than the 5<sup>th</sup> day of month for the

**FOR OFFICIAL USE ONLY**

preceding quarter/ month, (e.g., first quarter report is due NLT 5 January, 2d quarter report is due NLT 5 April, 3d quarter report is due 5 July).

**(2) HQ USEUCOM ECSM**

(a) Act as Office of Primary Responsibility for managing the CbTRIF program in USEUCOM.

(b) Assist in preparing any requests for USEUCOM DRUs and other non-component elements. Submit these requests in compliance with program guidelines, to include obtaining documentation of non-availability of funds from Defense Agencies.

(c) Upon receipt of requests, ECSM will:

- (1) Review project submissions to ensure that they meet CbTRIF criteria.
- (2) Prepare and submit staffing information packets on submitted

projects.

(3) Submit the requests to USCINCEUR or DCINCEUR for approval as USEUCOM funding nomination.

(4) Forward approved nominations to the Joint Staff (J-34) for action.

(5) Provide the requesters information on the status of requests.

(6) In coordination with ECCM, prepare a quarterly report to the CJCS outlining status of funded projects, benefits derived from the fund, obligation status and other issues and concerns relating to the fund (Tab B to this appendix) until completion of the project. Report the obligation status based on service component and/or local accounting system data. The report is due to J-34 by the 15th of the first month of each quarter (October, January, April, and each month of final quarter of the FY). Provide a information copy of this report to ECCM.

(7) Prepare a "Determination and Findings" statement in accordance with the Federal Acquisition Regulation, Part 17.5, for approved projects if funds are to be provided to a non-DoD activity.

**(3) HQ USEUCOM ECCM**

(a) Review all CbTRIF requests received from ECSM prior to submission to the Joint Staff.

(b) Determine that all requests meet funding statutory requirements.

(c) Validate sources and uses of funds.

(d) Determine the feasibility of using alternate sources of funds.

(e) Serve as the conduit for funding issues between HQ USEUCOM and Joint Staff.

**FOR OFFICIAL USE ONLY**

**(4) HQ USEUCOM ECJA.** Review all requests and proposals for the use of CbTRIF before such proposals are submitted to the Joint Staff.

**c. Coordinating instructions**

**(1)** Candidate initiatives for funding under the CbTRIF program may be submitted throughout the fiscal year in the format shown in Tab A to this Appendix.

**(2)** The fund is not intended to subsidize ongoing projects. Project submissions, either to cover shortfalls in funding or supplement a budget shortfall in a given project, normally will not be supported.

**(3)** CbTRIF projects that support routine activity or replace/upgrade/expand an existing security system/measure normally will not be supported. In addition, security equipment maintenance and repair is a Service responsibility and should be programmed accordingly.

**(4)** CbTRIF normally does not cover the leasing of equipment.

**(5)** Service component commands and DRUs may request CbTRIF money to fund requirements arising in the USEUCOM AOR. USCINCEUR may submit requests from non-CINC assigned commands if USCINCEUR has security responsibility or is enforcing USCINCEUR AT/FP standards upon the non-CINC assigned command element. USEUCOM will collate and prioritize requests and forward them to the Joint Staff (J34).

**(6)** Initiative requests approved in one fiscal year normally are not considered eligible for resubmission or follow-on funding in subsequent years. For this reason, the fund will not apply to civilian personnel positions. O&M appropriated funding for approved projects must be obligated before the end of the fiscal year for bona fide needs of that fiscal year. Procurement appropriated funding for approved projects must be spent in the same year it is received.

**(7)** Initiative requests are limited to O&M and procurement applications for security equipment, purchases, and minor construction. Use of O&M funds must not exceed the following thresholds: \$100,000 for systems, and \$1M for life threatening minor construction projects on any one installation. Projects exceeding these thresholds require procurement funding.

**(8)** Examples of possible uses of funds are listed below. Service component command candidate initiatives should be screened against this list to avoid ineligible projects from consideration before submission to higher authority. (Submit any inquires as to eligibility through the chain of command.)

**D-3-3****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

(a) Physical security equipment. Examples include surveillance systems, lighting, access controls, alarm systems, body armor, and vehicle armor kits.

(b) Physical security site improvement. Examples include minor construction, including perimeter and entrance barriers, fencing, and gates.

(c) Under extraordinary circumstances, component commands may submit requests for management and planning, security forces/technicians, and security and investigative matters. Examples of these include contract manpower, vulnerability assessments (TDY and equipment) associated costs, and training. CbTRIF will not be used to fund civilian or military personnel positions.

(9) USCINCEUR or DCINCEUR are the approving authorities for requests submitted by HQ USEUCOM to the CJCS.

**ACKNOWLEDGE:**

**JOSEPH W. RALSTON**  
General, USAF

**TABS:**

- A. CbTRIF Submission Format
- B. Quarterly CbTRIF Report Format
- C. Monthly Obligations Status Report

## FOR OFFICIAL USE ONLY

### TAB A (CbTRIF SUBMISSION FORMAT) TO APPENDIX 3 (COMBATING TERRORISM READINESS INITIATIVES FUND) TO ANNEX D (LOGISTICS) TO USCINCEUR AT/FP OPOD 01-01

#### Example of CbTRIF Request

1. **Submitted by:** CINC, Component Command and Parent Service
  - Operating Agency Code (OAC): Command the funds will be transferred to.
  - Approving Authority: Component Commander or Deputy/Vice Commander
2. **Point of Contacts:** Project POC: Name, Rank, Office, Phone #, Fax #, E-mail.  
Comptroller POC: Name, Rank, Office, Phone #, Fax #, E-mail
3. **Copy to Service HQ:** Date and method of submission to the Service
4. **AT Plan:** Does the requestor have an approved, executable, and exercised AT Plan? If yes, what is the date of the plan? If no, requests are not eligible for funding, unless plan is not executable due to requested item.
5. **Location:** Provide city and country of the unit/installation and the current Force Protection Condition.
6. **Type of Request:**
  - a. **(Emergency or Emergent)**
  - b. Why was the project not funded last year or budgeted for this year?
  - c. Confirm that the request is not for the purpose of subsidizing an ongoing project, supplements a budget shortfall, or support routine activity that is normally a Service responsibility.
7. **Requirement Generation:** **Identify** how the requirement was generated and recommended (JSIVA, Service VA, CINC VA, MACOM/MAJCOM, Echelon-2 IVA, self assessment, AT Plan development, exercise), and the date (month/year) the last assessment was conducted.
8. **Project Title:** (Unclassified version) and Component Project Control Number
9. **Project Description:** Define requirement to include:
  - a. Detailed description of the initiative, i.e., what the funds will purchase followed by a brief summary of what is to be accomplished.

## FOR OFFICIAL USE ONLY

**b.** Explain the specific type and application of physical security equipment (blast mitigation, communications, explosive detection, barriers, intrusion detection, personal protection or other special equipment/sensors) and/or physical security site improvements and facility modifications. Refer to basic document, definitions (paragraph 4).

**c.** Include applicable standards, regulations, and plans on which the requirement is based.

**d.** If applicable, describe steps taken to ensure technology requested will meet requirement.

**10. Justification:** State how the project directly supports CINCEUR's efforts to combat terrorism and justify the requirement through of four elements: Threat assessment, asset criticality assessment, vulnerability assessment, and AT plan/program effectiveness.

**a. Threat**

**(1)** State the threat level (High – Significant – Moderate – Low) based upon the DIA or CINC determination to assess the terrorist threat to DoD personnel

**(2)** Describe the specified threat (small/large bomb, WMD, etc.) to be defended against. Specific Threat Level information and guidance can be found in DoD 0-2000.12-H, Chapter 5.

**b. Asset Criticality.** Explain the asset (personnel/facility) criticality as it relates to the threat and the three facets below:

**(1) Importance.** Importance measures the value of assets located in the area, considering their function, inherent nature, and monetary value, if applicable.

**(2) Effect.** Effect measures the ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

**(3) Recoverability.** Recoverability measures the time it takes for the function occurring at that area to be restored, considering the availability of resources, parts, expertise and manpower, and redundancies.

**c. Vulnerability.** Explain the specific vulnerability as it relates to the specified threat (small/large bomb, WMD, etc.) and the asset mentioned above and the three facets of vulnerability:

**(1) Construction.** Construction measures the degree to which the area protects the assets within it from the effects of a terrorist incident.

**D-3-A-2**

**FOR OFFICIAL USE ONLY**



## FOR OFFICIAL USE ONLY

**(2) Accessibility.** Accessibility is measured in terms of the relative ease or difficulty of movement for terrorist elements and the likelihood of detection.

**(3) Recognizability.** Measures the degree to which a terrorist can determine the function and importance of an area and/or the assets located within it.

**d. AT Plan Effectiveness.** Describe the specific AT program shortfall to determine how effective the installation performs the AT functions related to addressing the terrorist threat using one or more of the following facets:

**(1) Policy/Procedures/Plans.** Measures the presence of effective plans, MOAs/MOUs and other agreements, as well as procedures for effectively performing the function.

**(2) Equipment.** Measures the adequacy of equipment used to perform the function. Consider whether the equipment is working properly, maintained properly, if there is a sufficient amount of equipment or if the equipment is obsolete.

### 11. Commanders Risk Assessment (CRA)

**a.** Based on the four elements (threat, asset criticality, vulnerability, AT Plan effectiveness) contained in the Justification Section (#10), state a rating of High (H) - Medium (M) - Low (L) for the Commander's risk assessment and provide rationale for the rating.

**b.** Describe the impact if the requirement is not funded this year.

**c.** Explain the current tactics, techniques, or procedures in place to address the vulnerability and why they are inadequate measures to mitigate the vulnerability.

**12. Priority:** Prioritize each requirement based upon the justification (threat, criticality vulnerability, the AT plan effectiveness (described in #10) and the Commanders risk assessment. The priority should be labeled as must (M), or need (N) in accordance with the following guidelines:

**Must: A required resource to mitigate a major risk**

**Need: A required resource to mitigate medium risk**

**13. Coordination:** Have the comptroller and legal counsel approved the request(s)? Have other sources of funding been pursued (e.g. contingency operations funding, Service channels)? If not, state the reason. If yes, state the reason they were denied.

### 14. Budgeting/Programming Information

D-3-A-3

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

- a. Are the requirements, and the life cycle costs, also being forwarded as an unfunded requirement through the Planning, Programming, and Budgeting System of the parent Service or CINC? If so, what is the specific control number of the project?
- b. What are the manpower and maintenance costs associated with this request? If additional costs are required, identify the requirement (e.g. replacement or shelf life) and what the anticipated cost is per year and for how many years.
- c. Identify how the follow-on sustainment costs will be funded: internal to the organization or Component command, or forwarded as an unfunded requirement with the applicable parent Service and/or CINC.
- d. If purchasing via contract, have the maintenance costs for the current year + 1 stop-gap year been built into the contract? This is common practice.

### 15. Current Fiscal Year Funding Plan

a. **Appropriation:**

**Amount Requested O&M/:** (Rounded to the nearest thousand)

**Amount Requested Procurement:** (Rounded to the nearest thousand)

b. **Amount Requested:** (Detailed cost estimates should be listed in this section. In particular, contractual services and equipment purchases must provide detailed unit costs, rates, and descriptions, to include contractual vehicles and acquisition contracts to be used. Identify any maintenance/sustainment costs required for the item and to be funded via CbT RIF. Also, identify any administrative pass-through costs charged to execute a contract.

**Example:**

<u>Item/Description</u>	<u>Cost/Unit</u>	<u># Requested</u>	<u>Total</u>	<u>Appropriation</u>
Hydraulic Barriers	\$2,000	4	\$8,000	O&M
Intrusion Detection	\$25,000	1	\$25,000	O&M
Notification System	\$1.4M	1	\$1.4M	Procurement
		Total:	\$33,000 - O&M	
			\$1,400,000 - Procurement	

D-3-A-4

FOR OFFICIAL USE ONLY

## **FOR OFFICIAL USE ONLY**

### **NOTES:**

- 1.** Adequate information is required in order for the HQ USEUCOM/ECSM to assess and prioritize each initiative competitively. Because of the length, submission by letter vice message is preferable.
- 2.** Submissions must contain all paragraphs and required information. Failure to provide correct information may result in processing delays and deferred requests until the appropriate information is provided.
- 3.** All submissions **MUST** be in the Vulnerability Assessment Management Program (VAMP) as validated, prioritized vulnerabilities. Submissions will not be considered unless identified and scored in the VAMP.

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**D-3-A-6  
FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

**TAB B (QUARTERLY CbTRIF REPORT FORMAT) TO APPENDIX 3 (COMBATING TERRORISM READINESS INITIATIVES FUND) TO ANNEX D (LOGISTICS) TO USCINCEUR AT/FP OPORD 01-01**

### Example of Quarterly CbTRIF Status Report

**Submitted by:**

**Amount funded:**

**Title:** (Unclassified version)

**Status of Project:** (Outline how the project was completed. If not complete, state what progress is being made and the expected completion date.)

**Funding Data:** (Indicate how much of the fund has been committed and provide a brief summary of how the fund has been obligated, name of contractor, vendor, or organization.)

**Benefits Derived:** (If project is complete, outline what benefits are being achieved.)

**Action Officer:** (Name, Rank, Office, Phone Number)

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**D-3-B-2**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**TAB C (MONTHLY OBLIGATIONS STATUS REPORT) TO APPENDIX 3  
COMBATING TERRORISM READINESS INITIATIVES FUND) TO ANNEX D  
(LOGISTICS) TO USCINCEUR AT/FP OPORD 01-01**

**CLASSIFICATION:** (As appropriate)

**COMBATING TERRORISM READINESS INITIATIVES FUND (CbTRIF)  
FY \_\_\_\_\_ OBLIGATIONS STATUS REPORT  
(Whole Dollar Amounts)**

**Component Command:  
Status as of:**

Total Allocated Funding:

Data per Accounting Records

<u>Release Increment/ Date _____</u>	<u>Gross Committed</u>	<u>Obligations</u>	<u>% Ob'd</u>	<u>Balance Unobligated</u>	<u>Projected Date 100% Obligations</u>	<u>Remarks</u>
--	----------------------------	--------------------	---------------	--------------------------------	--	----------------

Allocation #1  
(Dollar amount)

Allocation #2  
(Dollar amount)

Totals: \_\_\_\_\_

**POC:** Name  
Office  
DSN:                      FAX:  
E-mail address:

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**D-3-C-2**  
**FOR OFFICIAL USE ONLY**



## FOR OFFICIAL USE ONLY

### APPENDIX 4 (COMBATING TERRORISM TECHNOLOGY REQUESTS) TO ANNEX D (LOGISTICS) TO USCINCEUR AT/FP OPOD 01-01

<b>REFERENCES:</b>	CJCSI 5262.01, Combating Terrorism Technology Request Process
--------------------	---

**1. PURPOSE.** This appendix establishes policy and procedures for requesting Office of the Secretary of Defense (OSD) controlled research, development, test, and evaluation (RDT&E) for potential materiel solutions to command-identified, high priority, combating terrorism (CbT) deficiencies. The USEUCOM program is based on guidance in the CJCSI 5262.01, Combating Terrorism Technology Request Process.

#### **2. POLICY**

**a.** The CbT technology request process enables field commanders at the CINC, Service, component command, and facility levels to solicit commercial off-the-shelf (COTS) testing or rapid prototyping (RP) of potential materiel solutions from the Physical Security Equipment Action Group (PSEAG) and/or the Technical Support Working Group (TSWG), as applicable.

**b.** Requests must directly support Antiterrorism/Force Protection (AT/FP) for DoD personnel, their family members, DoD facilities, and DoD equipment.

**c.** The goal of the technology request process is to identify needed AT/FP capabilities; determine whether COTS options exist or whether technology is mature enough to support RP; test the option(s) if warranted; and provide product capability information to field commanders. Then, based on the threat, acceptable risk, and affordability, field commanders should purchase the option that satisfies their immediate needs.

**d.** If the TSWG or PSEAG cannot identify or provide potential options, then the deficiency must be addressed through the Service's requirements generation process. Thus, the secondary goal is to aid the Services in identifying CbT deficiencies that are systematic and require a permanent solution.

#### **3. The four phases of the Technology Request Process are:**

##### **a. Discovery.**

**(1) Identification.** Field commanders identify deficiencies or AT/FP capabilities that stem from changes in the terrorist threat, political situations, doctrine, and vulnerability assessments. Commanders then determine if a solution is materiel or technological, or if it is non-materiel such as procedures, policy, or personnel.

## FOR OFFICIAL USE ONLY

**(2) Determination.** If a materiel solution is warranted, field commanders should consult the Force Protection and Physical Security Equipment Technology Guide. This guide describes commercially available AT/FP equipment and points of contact. The guide is available on the Internet at <http://www.csc.com/pseag> and the Joint Staff J34 Homepage on the SIPRNet at <http://www.nmcc.smil.mil/j34/terrorism/index.html>. Another resource is the video compendium of products available through the Service component command AT/FP offices.

**b. Documentation.** When field commanders are unable to find a suitable option, they should request assistance from the PSEAG and TSWG, through their Service component command headquarters. Direct Reporting Units should forward their requests directly to HQ USEUCOM ECISM, and Defense Agency elements should forward their requests to their parent headquarters.

**c. Coordination.** The parent Service will send the request to the Force Protection Executive Action Group (FPEAG). An information copy of all requests generated within USEUCOM should be sent to HQ USEUCOM ECISM who in turn will forward a copy to the Joint Staff J34 within 14 calendar days, attaching any pertinent information to the request packet. A request from the field should take no longer than 30 calendar days to reach the FPEAG for action.

**d. Action.** The FPEAG prioritizes requests based on threat, date of submission, and other considerations and then submits the request to the PSEAG or TSWG, as applicable. The PSEAG or TSWG will develop solutions and/or provide options. When the PSEAG or TSWG cannot identify solutions or provide options, field commanders should pursue a solution through the parent Service's requirements generation process.

### 4. Technology Request Format

**a. Mission Deficiency and Threat Assessment.** Describe the mission deficiency and the factors influencing the deficiency in operational terms (i.e., what capability is needed and what crisis, AT/FP situation, or threat does this request address?). Describe the effectiveness of existing capabilities. If no capability exists, then so state. Indicate the fielding date desired and impacts to personnel safety and survivability if not fielded

**b. Potential Materiel Alternatives.** Identify any products that address similar needs. The products could be in development, in production, or deployed by other Services, Federal agencies, or allied nations. Market research on the part of the initiating or coordinating agencies is not required, simply an awareness of a potential product. State "NONE" if there are no known alternatives.

**c. Performance Parameters.** Identify operational performance parameters and other considerations that may impact the potential capability. Indicate if assistance is needed in identifying performance parameters.

D-4-2

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

**d. Funding.** State whether the responsible Service is willing to procure the requested capability and, if so, is there full or partial funding? Estimate the maximum O&M tail that can be afforded to support the system. If funding or offset is not available, so state. (This information usually will be provided by the Service component command or the parent Service.)

**e. Point of Contact (POC).** The requester should identify at least one POC familiar with the project. Provide rank, name, office symbol, DSN phone number, commercial number, e-mail address, and FAX number.

**f.** Format for the request is found at Tab A to this Appendix.

### ACKNOWLEDGE:

**JOSEPH W. RALSTON**  
**General, USAF**

### TAB:

A. Combating Terrorism Technology Request Format

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**D-4-4**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### TAB A (COMBATING TERRORISM TECHNOLOGY REQUEST FORMAT) TO APPENDIX 4 (COMBATING TERRORISM TECHNOLOGY REQUESTS) TO ANNEX D (LOGISTICS) TO USCINCEUR AT/FP OPOD 01-01

<b>REFERENCES:</b>	CJCSI 5262.01, Combating Terrorism (CbT) Technology Request Process
--------------------	---

**CbT TECHNOLOGY REQUEST  
FOR  
(TITLE OF OPERATIONAL CAPABILITY NEED)  
(Date of Request)**

- 1. Mission Deficiency And Threat Assessment.** Describe the mission deficiency and the factors influencing the deficiency in operational terms (i.e., what capability is needed and what crisis, CbT situation, or threat does this request addresses?). Describe the effectiveness of existing capabilities. If no capability exists, then so state. Indicate the fielding date desired and impacts to personnel safety and survivability if not fielded by the specified date.
- 2. Potential Materiel Alternatives.** Identify any products that address similar needs. The products could be in development, in production, or deployed by any Service, other Federal agency, or allied nation. Market research on the part of the initiating or coordinating agencies is not required, simply an awareness of a potential product. State "None," if there are no known alternatives.
- 3. Performance Parameters.** Identify operational performance parameters and other considerations that may impact the potential capability. Indicate if assistance is needed in identifying performance parameters. Enclosure D provides a guide to help determining specific performance parameters and environmental effects that impact on potential options.
- 4. Funding.** State whether the responsible Service is willing to procure the requested capability and, if so, is there full or partial funding? Estimate the maximum O&M tail that can be afforded to support the system. If funding or offset is not available, state so in this paragraph.
- 5. Point Of Contact (POC).** Identify at least one POC familiar with the request. Provide grade, name, office symbol, DSN number, commercial number, E-mail address, and fax number.

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**D-4-A-2**  
**FOR OFFICIAL USE ONLY**

# FOR OFFICIAL USE ONLY

## ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPORD 01-01

### REFERENCES: See Basic Order

**1. SITUATION.** Numerous DoD elements, personnel and assets constantly transit, or are deployed within, the USEUCOM area of responsibility (AOR). For the purposes of this OPORD, these DoD elements, personnel and assets are collectively referred to as "in-transit forces". Such forces often are traveling or conducting missions in areas outside of U.S. controlled areas; thus, particular attention must be given to the threat and sometimes unique vulnerabilities confronting in-transit forces.

**2. MISSION.** To provide policy and guidance regarding Antiterrorism/Force Protection (AT/FP) requirements for DoD elements, personnel and assets transiting, or deployed to, the USEUCOM AOR.

### **3. EXECUTION**

#### **a. Scheme of support**

**(1)** The policy and guidance in this Annex is applicable to DoD elements, personnel and assets (to include aircraft and ships) under the security responsibility of USCINCEUR. Specific guidance regarding command and control arrangements, and the scope of the CINC's authority (TACON for force protection) is contained in paragraph 5 of this Order. In most cases, categories and identification of DoD elements and personnel under the security authority of USCINCEUR are specified country specific COM-CINC Memoranda of Agreement (MOA), which are available via the SIPRNet at the USEUCOM Force Protection homepage, <http://www2.eucom.smil.mil/hq/ecsm/MOA/moa.html>.

**(2)** Commanders with FP responsibility for a transiting force shall ensure the execution of pre-deployment AT vulnerability assessments prior to deployment to locations where the Terrorism Threat level is Significant or High, or where a geographically specific Terrorism Warning Report is in effect. This includes movement routes that may be used by transiting DoD forces, ships and aircraft.

**(a)** Assessments of ports and airfields will be accomplished for DoD ships and aircraft IAW the Appendices to this Annex regardless of the threat level. Component commanders and supporting CINCs may waive these requirements for deployments and/or visits to DoD controlled locations such as existing military installations or ships afloat. 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.

## FOR OFFICIAL USE ONLY

**(b)** Transiting forces for the purpose of this Annex include all DoD ships and aircraft, and DoD units that could present lucrative terrorist targets, minimally those units or groups consisting of more than 50 personnel. Commanders may lower this threshold of unit size at their prerogative.

**(c)** Since a variety of factors could impact 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, 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.

**(3)** The Appendices to this Annex outline policies and processes for assessments of airfields, ports, and ground locations. Previous and periodic assessments of many locations will be available to commanders. These assessments may satisfy many pre-deployment assessment requirements and provide data that can be updated and/or validated to alleviate the need for an additional assessment, and reduce the scope of the assessment if it is warranted.

**(4)** Deploying commanders shall implement appropriate AT measures to reduce risk and vulnerability. If warranted, commanders faced with emergent AT/FP requirements prior to movement of forces should submit Chairman Combating Terrorism Readiness Initiatives Fund (CbT RIF) requests through established channels to procure necessary materials or equipment for required protective measures.

**(5)** Equipment and technology can significantly enhance AT/FP for all DoD forces, and in particular, the security posture of transiting units against terrorist threats. For this reason, component commanders should research and identify AT equipment and/or technology requirements to their chain of command. The use of commercial-off-the-shelf (COTS) or government-off-the-shelf (GOTS) products should be stressed to meet near-term requirements.

**(6)** A security plan for each deployment should be prepared, and while not to the detail of an installation AT/FP plan, should address the following areas:

- (a)** Task Organization
- (b)** Threat Assessment Process
  - (1)** Request and Review of Tailored Threat Information
  - (2)** Process and Equipment to Transmit and Receive Intelligence
- (c)** Vulnerability Assessment Process
- (d)** Concept of Operations
- (e)** Risk Assessment Process
- (f)** Random Antiterrorism Measures (RAM)



## FOR OFFICIAL USE ONLY

- (g) Implementation of Force Protection Condition Measures
  - (1) Security Measures Tailored to Local Conditions
  - (2) Transitioning to Higher Force Protection Condition
- (h) Physical Security Measures
- (i) Response and Consequence Management
- (j) Billeting Security (when applicable)
- (k) Access Control Procedures
- (l) Vetting of Contract Services
- (m) Local/Host Nation Support and Coordination

### b. Tasks and Responsibilities

#### (1) Component commanders

(a) Establish policies, as required, to ensure compliance with DoD and USCINCEUR requirements for in-transit security of units and personnel for whom the component commander has force protection responsibility. Working in conjunction with HQ USEUCOM, the following component commands will act as the lead executive agency for developing AT/FP guidance for in-transit forces:

- (1) **HQ USAFE** - Security for In-transit aircraft (Appendix 1)
- (2) **HQ USNAVEUR** - Security for In-transit ships (Appendix 2)
- (3) **HQ USAREUR** - Security for In-transit ground forces (Appendix 3)

(b) Establish Threat Working Groups (TWG) or comparable forum. The role of a TWG is to review intelligence and vulnerability assessment 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. Organizations with existing forums, which satisfy the role of a TWG, may continue to use that process and do not need to create a TWG, or rename any existing group. Specific tasks for a TWG are contained in selected Appendices and Tabs to this Annex.

(c) Ensure all assigned and/or attached personnel receive Level I AT/FP training and country/local area terrorist threat briefing or information prior to deploying or traveling to or within the USEUCOM AOR. In case of a no-notice deployment, units must give or coordinate for Level I training and country/local area terrorist threat briefings or equivalent information at the earliest opportunity after deploying.

(2) **All Theater Clearance Approval Authorities.** Under normal circumstances, do not grant theater clearance to any DoD element or individual deploying to this AOR unless certification is obtained validating that all deployed personnel have received required Level I AT/FP training and country/local area terrorist threat briefings or equivalent information. Additionally, verify that TDY/TAD orders identify the authority

## FOR OFFICIAL USE ONLY

responsible for security (either the CINC or the COM) and the local point of contact (POC) for AT/FP matters (as required by the DoD/DOS Universal MOU, reference (f)).

### **(3) HQ USEUCOM ECSM**

**(a)** Ensure the standards in this Annex are consistent with and satisfy DoD, CJCS, Service, and USCINCEUR AT/FP requirements. Promulgate theater AT/FP policy for in-transit forces, establish mechanisms to resolve security issues, and develop coordination procedures with DOS and country teams. Serve as USCINCEUR interface between DoD and DOS elements as needed.

**(b)** Coordinate as required with the appropriate agencies, e.g., DOS, DoD, Joint Staff, Defense Attachés (DATT), U.S. Defense Representatives (USDR), U.S. Embassy Regional Security Officers (RSO)) to ensure USCINCEUR security requirements are understood and addressed.

**(c)** Serve as the primary USEUCOM POC for communicating AT/FP policies and requirements for in-transit forces with the agencies listed in paragraph 3b(3)(b), above, and others as appropriate.

### **(4) HQ USEUCOM ECJ1**

**(a)** Act as the HQ USEUCOM staff proponent for establishing policy and procedures in the Foreign Clearance Guide to assist in tracking DoD elements and personnel TDY within the USEUCOM AOR.

**(b)** In coordination with the Service component command Personnel Directorates, ensure all PCS and TDY orders for personnel stationed in USEUCOM indicate the requirement for Level I AT/FP training.

**(c)** Require theater clearance approvals and TDY orders to specify the authority responsible for security, either USCINCEUR or the appropriate COM as well as the local AT/FP POC for personnel TDY within the theater.

### **(5) HQ USEUCOM ECJ2**

**(a)** Provide focused and tailored terrorist threat information to DoD elements and personnel deploying to, or transiting the USEUCOM AOR.

**(b)** Establish policies and procedures to require component command counterparts to disseminate focused and tailored terrorist threat information to all DoD elements and personnel deployed in support of the component commands, or transiting the AOR. Responsibilities should be divided and aligned along the functional lines in paragraph 3b(1)(a), above.

## FOR OFFICIAL USE ONLY

**(6) HQ USEUCOM ECJ3.** In coordination with ECSM, ensure that AT/FP is factored into all aspects of mission planning and execution. Conduct risk assessment as required to ensure adequate AT/FP is in place prior to the execution of USEUCOM-directed missions.

### **(7) HQ USEUCOM ECJ4**

**(a)** Assist ECJ3 in tracking the deployment and movement of logistics support forces and materiel throughout the theater.

**(b)** Ensure AT/FP requirements are included in all aspects of planning and execution for the movement of logistics support within the theater.

**(8) HQ USEUCOM ECJ5.** Facilitate coordination with U.S. Defense Representatives (USDR) regarding USCINCEUR policies for approving theater country clearance requests for distinguished visitors to Africa and the Middle East, and ensure CINC policies are strictly adhered to.

### **(9) HQ USEUCOM ECJ6**

**(a)** Coordinate as appropriate to ensure adequate communications capabilities exist for deployed and in-transit forces.

**(b)** Resolve information security policy issues impacting on AT/FP capabilities of deployed or in-transit forces.

### **(10) HQ USEUCOM ECS0**

**(a)** Track the movement of all DoD elements and personnel conducting special operations missions within the USEUCOM AOR.

**(b)** In coordination with ECJ2, ensure that focused and tailored terrorist threat information is disseminated to all in-transit forces supporting special operations missions.

### **(10) Parent Organizations of In-Transit Forces**

**(a)** Track the movement of all in-transit subordinate elements and personnel within the USEUCOM AOR.

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

**(c)** Require assigned in-transit forces to engage in the risk assessment management process prior to deploying to, or within, the USEUCOM AOR.

## FOR OFFICIAL USE ONLY

### c. Coordinating instructions

(1) Every deployment must be provided with a focused, tailored threat assessment that reflects the most up to date threat information and the impact on the threat environment of raising the profile of U.S. personnel due to the deployment. A generic threat assessment may change once the increased presence of U.S. forces on the ground is factored in. This threat assessment is a stand-alone product that should include the information similar to that gathered for the Risk Assessment Management Program (RAMP) system.

(2) The supporting intelligence center/element must coordinate for additional collection emphasis for certain deployments. This will ensure additional collection is dedicated to meeting the force protection needs of deploying and in transit forces.

(3) As applicable, commanders also will ensure compliance with requirements of Appendix 1 to Annex C (Pre-Deployment Requirements) and Tab A to Appendix 1 to Annex C (Training and Equipment Requirements).

### ACKNOWLEDGE

**JOSEPH W. RALSTON**  
General, USAF

### APPENDICES:

1. Security for In-transit Aircraft
  - TAB A: Coordinated Transient Aircraft Security Requirements
  - TAB B: Message Guidance for Requesting Additional Security
  - TAB C: Rules of Engagement/Use of Force
  - TAB D: Threat Working Group
  - TAB E: Airfield Responsibility Matrix
  - TAB F: Airfield Assessment Checklist
2. Security for In-transit Ships
  - TAB A: Example of Inport Security Plan
  - TAB B: Example of LOGREQ Security Supplement
  - TAB C: Example of Inport Security Plan Approval
  - TAB D: Security Assessment Survey Form and Checklist for Non-U.S. Ports
3. Security for In-transit Ground Forces
  - TAB A: Assessment Checklist for In-transit Ground Forces

# FOR OFFICIAL USE ONLY

## APPENDIX 1 (SECURITY FOR IN-TRANSIT AIRCRAFT) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPORD 01-01

### REFERENCES: See Basic Order

**1. PURPOSE.** To provide transient aircraft and accompanying personnel adequate security within the USEUCOM AOR, to include the Russian Federation west of 100° East.

**2. APPLICABILITY.** This Annex applies to all DoD aircraft and accompanying personnel operating in the USEUCOM AOR under the Antiterrorism/Force Protection (AT/FP) responsibility of USCINCEUR.

### 3. POLICY

**a.** It is the policy of USCINCEUR to deter terrorism through the use of all reasonable means. While reducing the risk to DoD resources from acts of terrorism is a command responsibility, each person in the USEUCOM AOR must exercise proper caution and prudent judgment to reduce their own vulnerability.

**b.** Each USEUCOM activity and all DoD aircraft and personnel for whom USCINCEUR has AT/FP responsibility must establish subordinate policies based on this order, tailored to mission and local conditions. To achieve this objective, USCINCEUR directs the use of the USAFE Risk Assessment Management Program (RAMP) 2.0 at <http://coldfusion.ramstein.af.smil.mil/RAMP/index.cfm> and the USAFE Logistics Plans Site Survey Information web page for airfield information. The web page is located on SIPRNET at <http://www.ramstein.af.smil.mil/Logistics/bsp.html>. HQ USAF has mandated the use of the Employment Knowledge Base (EKB) immediately upon data population. Expect the USAFE Logistics Plans web page to completely transition to the EKB NLT 2005. USAFE will continue to track the progress of the EKB and develop theater implementation instructions.

### 4. IN-TRANSIT AIRCRAFT SECURITY PROCEDURES

**a.** Designated component command agencies will prepare the flight operations advisory/diplomatic clearance message using the guidelines provided in Tab B to this Appendix.

**b.** Component commands must be able to maintain continuous contact with transiting aircraft. Component commands will identify shortfalls in en route communications capabilities and will take steps to aggressively pursue the ability to contact aircraft, en route, anywhere in the USEUCOM AOR. Inability to satisfy this requirement will be reflected in executive/operations orders and considered during

## FOR OFFICIAL USE ONLY

mission planning/approval, but does not require submission of a waiver request to HQ USEUCOM.

**c.** Component commands and Task Force commanders will conduct airfield security/vulnerability assessments and are responsible for airfield Risk Assessment Management Program (RAMP) database entries. Component commands will forward their assessments electronically to the USAFE Threat Working Group (TWG) for a quality control check prior to the component entering the data into the RAMP. Each component level headquarters and USAF main operating base (MOB) is responsible for establishing a TWG (or comparable working group), conducting airfield assessments, making RAMP database entries, and maintaining RAMP assessments for their own bases and locations for which they have been deemed responsible in accordance with the guidance below (see Tab E to this Appendix for a breakout of responsibilities for airfields). USAREUR and USNAVEUR will determine and document requirements for subordinate Working Groups, normally establishing these at all naval bases, ASGs, BSBs, and within Task Forces. MARFOREUR and SOCEUR should convene Working Groups prior to planned missions. The role of the TWG (or comparable working group) is to vet upcoming missions by viewing available intelligence and RAMP database information for in-transit locations prior to making risk management decisions on aircraft/troop movements. Although the specific designation for this working group may vary among the component commands, the term "component command TWG" will be used in this Appendix to refer to this functional entity.

**(1)** USAFE is responsible for conducting assessments on all USAFE controlled airfields (e.g., Aviano AB), fixed wing international/regional civilian airports used by USAF aircraft (e.g., Frankfurt IAP), and all other airfields at which USAF aircraft (fixed and rotary wing) operate or visit.

**(2)** USAREUR is responsible for conducting assessments on all Army Airfield-specific helipad/landing zones and fixed wing locations (e.g., Grafenwoehr AAF), as well as other locations at which U.S. Army aircraft (fixed and rotary wing) operate or visit, and are not otherwise included in the USAFE RAMP.

**(3)** USNAVEUR is responsible for conducting assessments on all Naval/Marine Corps-specific Air Stations and helipads/landing zones (e.g., Souda Bay NAS), as well as other locations at which U.S. Navy aircraft (fixed and rotary wing) operate or visit, and are not otherwise included in the USAFE RAMP.

**(4)** MARFOREUR is responsible for conducting assessments on locations at which U.S. Marine Corps aircraft (fixed and rotary wing) operate or visit, and are not already assessed by USNAVEUR or another component command.

**(5)** SOCEUR and JTFs are responsible for conducting assessments for airfields/helipads which they use or transit, and are not already addressed above.

## FOR OFFICIAL USE ONLY

**(6)** If a component command enters a new location into the RAMP based on Service requirements, or has a mission to an airfield that is not in the existing RAMP database, that component has the responsibility for developing the risk assessment, and ensuring the appropriate airfield security assessment is completed.

**(7)** For airfields used only by non-USCINCEUR DoD elements (e.g., TRANSCOM, USCINCENT), HQ USAFE will provide available airfield data to requestors. HQ USAFE will coordinate all airfield assessments through the appropriate U.S. Defense Representative (USDR). See paragraphs 4d and 4f, below, for assessment criteria guidance.

**(8)** Component commands proposing changes to the Assessment Responsibility Matrix (Tab E to this Appendix) will address their proposals to HQ USAFE as the USEUCOM executive agent for management of this program. Every effort will be made to resolve issues regarding responsibility through a process of coordination among the component commands. Disagreements over assessment responsibility, which cannot be resolved by HQ USAFE, will be addressed to HQ USEUCOM ECSM for resolution.

**(9)** To avoid duplication of effort when two or more component commands use a non-Service specific location, responsibility for conducting the assessment will generally follow in the order shown below for the component commands in question (See Tab E to this Appendix for current breakout of airfield responsibilities):

Fixed Wing Locations: USAFE, USNAVEUR, USAREUR,  
SOCEUR, MARFOREUR  
Rotary Wing Locations: USAREUR, USAFE, SOCEUR,  
USNAVEUR, MARFOREUR.

**d.** Assessment criteria will depend on the type of location.

**(1)** Annual vulnerability assessments which are performed by host units will suffice for U.S. installations (U.S. military controlled).

**(2)** Other Security Category "A" (CAT "A") airfields require an annual confirmation of adequate security presence and policies (see paragraph 5, below). This confirmation may be conducted by transiting forces (e.g., aircrews) and/or the U.S. Embassy DAO or Regional Security Officer (RSO) and should examine all aspects of security and safety using the Airfield Assessment Checklist (Tab F to this Appendix).

**(3)** Airfields designated Security Category "B" (CAT "B") require more stringent security/vulnerability assessments (see paragraph 6, below). An annual on-site assessment by a multi-disciplined team well versed in antiterrorism/force protection is required for CAT "B" airfields critical to wartime or contingency operations and/or CAT "B" airfields that large troop movements (50 or more) traverse at a single time. CAT "B" airfields not meeting the above criteria will also be assessed annually as well; however, the assessments may be conducted by transiting aircrews, security force personnel, or

**E-1-3**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

the U.S. Embassy RSO/DAO. Verification of the information should be conducted by aircrews and security force personnel accompanying each flight, time permitting. For CAT "B" airfields infrequently used, the annual assessment requirement may be postponed until such time a mission is planned to transit that location. In such cases, the assessment must be conducted prior to mission arrival and in sufficient time to allow mission vetting by the appropriate TWG. In all cases, the Airfield Assessment Checklist will, as a minimum, be completed. If a current assessment does not exist, the respective USEUCOM component commander or supporting CINC (e.g., USTRANSCOM) or their respective TWG will decide mission execution using available information and intelligence.

(4) The Component Command TWG will determine individual vice team requirements for initial assessments of airfields that are not critical to wartime or contingency operations and are not used for large troop movements. These assessments may be conducted by multi-discipline teams, individuals, or U.S. Embassy RSO/DAO. The TWG should consider the threat and status (CAT "A" or "B") of other assessed airfields in the country/region when determining initial assessment criteria.

(5) Regardless of the category type, mission planners, mission commanders, and TWGs must consider the frequency, type, and quality of security-related assessment information, as well as current threat, when making risk management decisions on aircraft movements.

e. As the executive agent for the airfield RAMP, HQ USAFE is the lead agency for USEUCOM in determining aircraft security and airfield risk assessment policies for transiting aircraft, to include deploying aircraft from CONUS and other geographic AORs. In this capacity, HQ USAFE will perform as liaison between the component commands (as listed in paragraph 4c, above); other CINCs, Services, and Defense Agencies; and other DoD/DOS elements as listed in paragraph 3b(3) of Annex E. This liaison authority does not include addressing policy issues with those elements listed in paragraph 3b(3) of Annex E. Initial communication/contact with a U.S. Embassy Country Team (usually the USDR) regarding in-transit aircraft security issues, including assessments, will be made by HQ USAFE, with subsequent communication made by the affected/responsible component command. The intent is to avoid duplication of effort, minimize unnecessary burdens on DoD/DOS agencies, and preclude tensions with host nation agencies and officials. HQ USAFE will notify the appropriate USDR and RSO of proposed assessment schedules, and request assistance when applicable.

f. USAFE TWG will ensure component commands responsible for conducting assessments adequately evaluate and categorize respective airfields into two categories (CAT "A" and CAT "B") based on location and security measures at those locations. Examples range from U.S. military controlled airfields to bare-base airfields. Disagreements between the HQ USAFE TWG and other component command TWGs over the CAT "A" versus CAT "B" decision will be referred to HQ USEUCOM ECSM for resolution.



## FOR OFFICIAL USE ONLY

- (1) CAT "A" airfields do not normally require additional security.
- (2) CAT "B" airfields normally require additional security.

CAT "A"	CAT "B"
U.S. military controlled	Non-NATO military controlled with inadequate or questionable security
NATO military controlled	International/Regional Airport with inadequate or questionable security
Non-NATO military controlled with adequate security confirmed	Bare base
International/Regional Airport with adequate security confirmed	Unknown/No data available

NOTE: Special circumstances, mission criticality, heightened Terrorism Threat Level, Defense Terrorism Warning Report issuance, or increased Force Protection Condition, may cause an airfield to move from CAT "A" to CAT "B" designation.

**5. TRANSIENT OPERATIONS TO SECURITY CAT "A" AIRFIELDS.** CAT "A" airfields, by definition, do not normally require security augmentation for routine operations under normal circumstances. Exceptions to this may occur in the event intelligence indicates a specific threat that indicates terrorist targeting of airfields or aircraft. Additional security should also be afforded for high visibility transits and those involving large-scale unit deployments. Security and planning guidance applicable to CAT "B" airfields should be incorporated on a case-by-case basis.

**6. TRANSIENT OPERATIONS TO SECURITY CAT "B" AIRFIELDS.** The following provides general policy for agencies and crewmembers as it relates to planning and executing aircraft security/force protection measures at CAT "B" 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.

### a. PRIOR TO DEPARTURE

(1) The aircrew must receive a tailored, comprehensive planning package that, beyond standard flight planning information, includes a summary of threats along the route of flight, the terminal area, and at the airfield itself. The package also will contain U.S. Embassy Country Team information to include RSO contact numbers/names, USDR, who usually is the Defense Attaché (DATT), contact numbers, and how to contact local/contracted security at the airfield of intended destination. Imagery of the airfield, if available, should indicate the likely parking location so that the aircrew can determine escape routes should that become necessary. The package should include the person or persons, by name, who will meet the aircraft in order to provide liaison and updates on security conditions as they exist at the time of arrival. If operating at a

## FOR OFFICIAL USE ONLY

civilian airfield, the package should include the name of the companies that will be providing aircraft servicing.

**(2)** If the airfield is designated in RAMP as a location requiring onboard security personnel to accompany the mission (Armed Escorts/Security Forces), the security members will receive the same information and 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 Use of Force and Rules of Engagement (ROE) (see Tab C to this Appendix). The designated component command element, TWG, or two-person security team (hereafter referred to as Security Team (ST) Leader and ST Member) will make contact with a member of the U.S. Embassy Country Team NLT 24 hours prior to departure for current airfield information. Component commands will determine the appropriate coordination procedures with Country Teams to ensure adequate exchange of information without unnecessary and redundant interactions.

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

**(4)** When the type or size of the aircraft does not permit on-board security personnel (and such support is identified as a requirement), the component command or supporting CINC will request additional Host Nation security support (see sample request at Tab B to this Appendix) or send advance U.S. security elements. When Host Nation support will still not satisfy DoD/USEUCOM requirements and U.S. provided security is not feasible, the respective TWG will advise the appropriate commander for a decision regarding execution of the mission.

**b. EN ROUTE.** From a force protection 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 late-breaking, updated threat information to its aircraft en route, possibly leading to an en route change of destination.

**c. ARRIVAL.** Normally, aircrews expect either a follow-me vehicle or directions from tower personnel, or a combination of the two, providing guidance to their designated parking location. For missions with additional security support on board, adhere to the following procedures:

**(1) Taxi to parking.** During taxi in, the two security personnel will position themselves in such a way as to scan the ramp area for suspicious personnel, vehicles, or activity. Country Team personnel (e.g., RSO/DAO) or designated/contracted security personnel will normally be requested to meet the aircraft. As the aircraft stops in parking, the aircrew will leave one engine or APU running while security personnel

## FOR OFFICIAL USE ONLY

deplane. Cockpit crewmembers will remain strapped in, poised to restart engine(s) to taxi away from the area, or even take off, if the situation warrants. ST Leader will observe ground personnel during chocking of the aircraft, positioning of power carts and fire bottles as appropriate. ST Member will scan the area while circling the aircraft. ST Leader will then meet with the local security representative where they should be briefed on the following:

(a) Status of airfield security.

(b) Means of calling for security/response, if it is required.

(c) Duress words to be used while the aircraft and crew is on station (when beneficial and reasonable).

(2) When ST Leader is satisfied with security, he will give a “thumbs up” to ST Member and the cockpit crew who can then shutdown the APU/engines and open the aircraft. ST Member will continue providing roving area surveillance while ST Leader and aircraft crewmembers supervise any additional ground support personnel and equipment needed to service the aircraft. (Note: Local country team personnel will need to brief local customs personnel of the above security teams' actions.)

(3) Before any service vehicle is allowed to pull up to/approach the aircraft, local security personnel, or aircrew members in their absence, will identify vehicle occupants and examine the vehicle for potential threats/hazards. At no time should an unexpected vehicle be allowed to come within 100-ft (35 m) of a DoD aircraft without being challenged, stopped, and examined.

(4) Upon completion of the arrival servicing sequence, the aircraft should be sealed if it is to remain overnight. For night or dusk/dawn operations, aircraft should be parked under adequate lighting allowing illumination of all four sides. All crewmembers, prior to departing from the airfield, should receive a complete brief by the local security representative on the current threat situation off the airfield (en route to their quarters, and the area where the crew will crew rest (sleep, eat, etc.)). All crewmembers should receive phone numbers for fire, police, hospital, ambulance, and U.S. government support representatives. They should also be briefed on particular areas and establishments to avoid which might pose a threat to the crewmembers.

**d. OFF AIRFIELD ACTIVITIES.** If crewmembers or passengers are to use rental vehicles, they should only be procured from a U.S. Country Team recommended/contracted dealer when such information is available. Prior to loading, starting, or driving the 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 the U.S. Country Team or local U.S. military officials, when such information is available, and should conduct inspections of their rooms using DoD approved checklists. Rooms should also be reexamined when returning and vehicles reexamined after being left unattended.

E-1-7

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

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.

**e. DEPARTURE.** The same basic procedures used in the arrival sequence will apply for departure. Security personnel will provide area surveillance and control access while the aircraft is prepared for departure. Once the engines are started security personnel will assume positions inside the aircraft to monitor the area for suspicious activity, personnel and equipment, until such time they are required to assume seat positions for takeoff. Either the security team or aircrew will submit a completed General Physical Security Checklist (Tab F to this Appendix), to the Component Command TWG, upon arrival at home station. Any new information on the airfield will be validated by the Component Command TWG and forwarded to the USAFE TWG electronically prior to the component command entering the data into the RAMP database. This should be accomplished within 72 hrs upon arrival at home station. Items of immediate concern should be relayed to the aircraft's assigned command and control agency as soon as possible (e.g., en route communications).

### ACKNOWLEDGE

**JOSEPH W. RALSTON**  
**General, USAF**

### TABS:

- A. Coordinated Transient Aircraft Security Requirements
- B. Message Guidance for Requesting Additional Security
- C. Rules of Engagement/Use of Force
- D. Threat Working Group
- E. Airfield Responsibility Matrix
- F. Airfield Assessment Checklist

## FOR OFFICIAL USE ONLY

### TAB A (COORDINATED TRANSIENT AIRCRAFT SECURITY REQUIREMENTS) TO APPENDIX 1 (SECURITY FOR IN-TRANSIT AIRCRAFT) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPOD 01-01

#### REFERENCES: See Basic Order

1. The responsible component command or supporting CINC will coordinate with the appropriate U.S. Defense Representative (USDR) and/or U.S. Embassy Regional Security Officer (RSO) to ensure the following security requirements are implemented at Security CAT "B" airfields. This normally will be accomplished via message traffic, and may be included in the theater/country clearance request message. HQ USEUCOM has provided these baseline standards to all USDRs and RSOs in the USEUCOM AOR.

a. Some form of unimpeded escort for the aircraft to and from designated parking location.

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

c. Host nation/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.

d. Host nation/contracted security forces prevent personnel or equipment from entering the security zone until cleared by a U.S. crewmember.

e. 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.

f. If the aircraft must RON, ensure the following additional measures are provided:

(1) A 24-hour manned entry 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).

(2) Arrange for lodging of crew at a DoD or DOS approved/recommended facility.

2. If security arrangements are deemed inadequate, or not in compliance with this annex, 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 command and control (C2) agency.

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**E-1-A-2  
FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### TAB B (MESSAGE GUIDANCE FOR REQUESTING ADDITIONAL SECURITY) TO APPENDIX 1 (SECURITY FOR IN-TRANSIT AIRCRAFT) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPOD 01-01

#### REFERENCES: See Basic Order

1. The following guidance/procedures shall be included in messages requesting aircraft support for all DoD aircraft missions to Security CAT "B" airfields within the USEUCOM AOR (this data may be included in standard diplomatic clearance message). The intent of these guidelines is to create a "U.S. Controlled Zone of Security" around these assets at all Security CAT "B" airfields.

#### SECURITY PARAGRAPH/SECTION

1. REQUEST VERIFICATION BE PROVIDED CONCERNING THE FOLLOWING AIRFIELD SECURITY MEASURES:

A. SECURE OPERATING ENVIRONMENT THAT PERMITS SAFE MOVEMENT OF THE AIRCRAFT DURING LANDING AND TAXI OPERATIONS TO/FROM DESIGNATED PARKING LOCATION.

B. AIRCRAFT PARKING LOCATIONS A MINIMUM OF 300 FEET (100 METERS) FROM THE AIRFIELD PERIMETER, BUILDINGS, OR OTHER NON-U.S. MILITARY AIRCRAFT ON THE RAMP.

C. HOST NATION/CONTRACT SECURITY FORCES PREPARED TO IMMEDIATELY ESTABLISH A SECURITY ZONE, ENCOMPASSING THE ENTIRE AIRCRAFT AT A MINIMUM DISTANCE OF 100 FEET (35 METERS) USING, IF AVAILABLE, ELEVATED ROPES/STANCHIONS OR SIMILAR EQUIPMENT. FOUR RESTRICTED AREA OR WARNING SIGNS WRITTEN IN THE LOCAL LANGUAGE(S) DISPLAYED ALONG THE PROPER BARRIER.

D. DEDICATED HOST NATION/CONTRACT SECURITY FORCES TO REMAIN IN CLOSE PROXIMITY TO THE AIRCRAFT AND PREVENT PERSONNEL OR EQUIPMENT FROM ENTERING THE SECURITY ZONE UNTIL CLEARED BY A U.S. AIRCREW MEMBER DURING ALL OPERATIONS TO INCLUDE REFUELING/SERVICE, ETC.

E. A SECURITY GUARD PRESENT AS AN AIRCRAFT ENTRY CONTROL POINT GUARD ON A 24 HR BASIS DURING THE ENTIRE GROUND TIME. THE GUARD MAY BE U.S. MILITARY, FOREIGN MILITARY, CIVIL/AIRPORT POLICE OR CONTRACT SECURITY. NOTE: THE PURPOSE OF THE GUARD IS TO PROVIDE ENHANCED SECURITY WITH IMMEDIATE ACCESS TO THE LOCAL SECURITY NETWORK AND TO ASSIST AIRCREW PERSONNEL IN CONTROLLING ACCESS TO THE AIRCRAFT. ANYONE NOT ON AN OFFICIAL PASSENGER MANIFEST OR

**E-1-B-1**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

CREW ORDERS WILL BE DENIED ENTRY WITHOUT THE AIRCRAFT COMMANDER'S OR MISSION CONTACT OFFICER'S APPROVAL.

F. SECURITY/ESCORTS ARE AVAILABLE TO SUPPORT AIRCREW AS FOLLOWS: (SPECIFY). DELETE THIS REQUIREMENT IF NOT APPLICABLE.

G. LIGHTING, IF REQUIRED, TO ADEQUATELY ILLUMINATE ALL FOUR SIDES OF THE AIRCRAFT AT NIGHT.

H. COMMUNICATIONS CAPABILITY (RADIO OR TELEPHONE) BETWEEN THE AIRCRAFT SENTRY AND THE EMBASSY OR AIRPORT POLICE HEADQUARTERS IF AIRCRAFT WILL REMAIN OVERNIGHT.

I. BILLETING ASSISTANCE FOR PERSONNEL AT DOD/DOS APPROVED/RECOMMENDED FACILITIES IF AIRCRAFT WILL REMAIN OVERNIGHT.

2. CHARGES FOR SERVICES WILL BE PAID BY CASH, OR UNDER THE SERVICES FUND CITE.

3. PLEASE PROVIDE A RESPONSE TO (UNIT OPR/DIPLOMATIC CLEARANCE AGENCY) NLT (DATE) AS TO WHICH MEASURES CAN AND WILL BE IMPLEMENTED. FOR ANY MEASURES THAT CANNOT BE PROVIDED, INCLUDE A DESCRIPTION OF ANY COMPENSATORY ACTIONS.

4. FUND CITE: FUEL, SERVICES, AND ADDITIONAL SECURITY: TBD

5. 24 HOUR NOTIFICATION AND (UNIT POC INFORMATION)

EXAMPLE:

USAFE AMOCC POC: SMGT JOHN SMITH, COMM TEL: 49-6371-47-6853 OR 49-6371-47-9292. DSN: 314 480-6853 OR 480-9292

UNCLASS FAX - COM: 49-6371-47-9811 DSN: 314 480-9811

E-MAIL: AMOCC.XOCG@RAMSTEIN.AF.MIL

SIPRNET E-MAIL:

6. REQUEST ACKNOWLEDGED RECEIPT OF THIS MESSAGE AND REQUIREMENTS.

REGARDS (UNIT OPR)

**E-1-B-2**  
**FOR OFFICIAL USE ONLY**



## FOR OFFICIAL USE ONLY

### TAB C (RULES OF ENGAGEMENT/USE OF FORCE) TO APPENDIX 1 (SECURITY FOR IN-TRANSIT AIRCRAFT) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPORD 01-01

**REFERENCES:** See Basic Order

**GENERAL:** The following is basic guidance for Rules of Engagement (ROE) and Use of Force.

1. DoD aircraft are sovereign instrumentalities. When cleared to over fly or land in foreign territory, it is U.S. policy to assert that military aircraft are exempt from duties and taxation and immune from search, seizure, inspection (including customs and safety inspections) and other exercise of jurisdiction by the host nation. Aircraft commanders (AC) and Security Team Members (ST Members) may not authorize the search, seizure, inspection or other exercise of jurisdiction by foreign authorities unless directed by the appropriate higher authority, e.g., Service headquarters or the local U.S. Embassy.

a. If foreign government or military officials attempt to force their way aboard DOD aircraft, STs should not physically restrain them unless they attempt to harm DoD personnel or property. The ST will contact the AC and local U.S. Embassy personnel immediately.

b. If foreign nationals, who are not military or governmental officials, attempt to enter a DOD aircraft without permission, ST Members may use appropriate force to resist. If this situation arises, ST Members contact the AC and local U.S. Embassy personnel immediately.

2. In general, whether inside or outside the aircraft, ST Members may use force according to CJCSI 3121.01, *Standing Rules of Engagement for U.S. Forces and appropriate component instructions*.

3. Inside the aircraft, an area of U.S. sovereignty, ST Members may apprehend and prevent the escape of a person who has committed an offense. Outside the aircraft, ST Members may not seek to apprehend or prevent the escape of a foreign national. This is considered a local law enforcement function and the responsibility of the host nation. ST Members should seek the assistance of host nation personnel in order to apprehend or prevent the escape of a foreign national who has injured or threatened to injure U.S. personnel or equipment on the aircraft.

4. At locations where security is not adequate and at ST required locations (STRL), two-person STs establish close-in security and remain with the aircraft at all times, unless otherwise directed by the aircraft commander.

5. ST Members must adhere to limitations relating to the wear of the uniform and arming restrictions outlined in the DoD 4500.54G, *Department of Defense Foreign*

**E-1-C-1**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

*Clearance Guide (FCG)*, Status of Forces Agreements (SOFA), NATO Standardization Agreements (STANAGs) and other applicable international agreements. ST Members should consult their servicing Staff Judge Advocate, as needed, for briefings on/interpretation of the applicable agreements and on arming and use of force considerations for mission locations prior to mission initiation.

**a.** ST Members posted in a guard capacity will be armed or an armed over watch will be present (subject to Host Nation limitations, SOFA, or contract limitations). Arming is defined as being in possession of a firearm and ammunition. Any firearms not carried on a person will be positioned where readily available should their use be warranted (proximate threat presents itself). Weapons retrieved from within an aircraft by unarmed guards to neutralize a threat should be returned to the aircraft as soon as possible. If a staged operation is being conducted and the weapons will be carried outside the aircraft, the aircraft's assigned command and control agency will be the focal point to coordinate weapon permits with the local U.S. Embassy at the location of concern.

**b.** Given that the threat to DoD assets can change quickly, there may be situations (local rioting, bombings, etc.) that warrant the removal of the weapons from the aircraft at a deployed airfield. In situations other than an immediate hostile threat to DoD assets, the AC commander or ST leader will contact the U.S. Embassy representative, e.g., Defense Attaché Officer (DATT) or Regional Security Officer (RSO), for authorization to remove weapons from the aircraft. The AC or ST leader also will contact their assigned command and control agency as soon as possible, to provide a detailed briefing of the current conditions.

**c.** After completing security coordination and prior to entering crew rest, upon receiving proper authorization per paragraphs 5a and b, above, the AC or ST leader will arrange to store all weapons and ammunition in a secure DoD, U.S. Embassy, or NATO armory (if Service regulations or directives permit such storage). If these facilities are not available, ST will store weapons and ammunition aboard the aircraft in a locked container (if Service regulations or directives permit such storage). Suggest securing weapons in a locked container that is properly secured to the aircraft, and that weapons and ammunition be stored in separate containers.

**6.** If a foreign national approaches an AC/ST member to request political asylum or temporary refuge, entry to the interior of the aircraft will not be permitted. AC or ST should refer immediately all situations of this type to the nearest U.S. Embassy or Consulate. The senior commander or AC may afford temporary refuge in order to secure the life or safety of the foreign national against imminent danger, but only to that extent consistent with the safety of the aircraft and U.S. personnel.

## FOR OFFICIAL USE ONLY

### TAB D (THREAT WORKING GROUP) TO APPENDIX 1 (SECURITY FOR IN-TRANSIT AIRCRAFT) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPOD 01-01

#### REFERENCES: See Basic Order

**PURPOSE.** Threat Working Groups (TWG) are required for each component command and subordinate organization, as directed in paragraph 3b(1), Annex E. The primary role of a multi-disciplined component command TWG is to vet upcoming missions by reviewing available intelligence and RAMP database information for in-transit locations prior to making risk management decisions on aircraft/troop movements. The TWG also ensures assessments are conducted IAW assessment policies in Annex E and appropriate information is forwarded to the USAFE TWG and/or entered into the airfield RAMP database. As the executive agent for the airfield RAMP, USAFE will have the lead for USEUCOM Commands/Services/Agencies/Activities in determining aircraft security and airfield risk assessment policies for transiting aircraft, to include deploying aircraft from CONUS and other geographic AORs.

#### GENERAL

##### 1. THREAT WORKING GROUP REQUIREMENTS

###### a. USEUCOM Responsibilities

(1) Coordinate airfield risk assessment issues between component commands and other CINCs/Services and DoD agencies.

(2) Engage, as necessary, with the respective U.S. Embassy country team officials to facilitate airfield assessments and security for in-transit aircraft and personnel.

(3) Advocate for the resources (manpower, funding, systems, etc.) necessary to conduct airfield risk assessments.

(4) Deviations from stated policy, except requirement for continuous contact with aircraft, must be submitted to USEUCOM Chief of Staff for approval.

###### b. USDR Responsibilities

(1) Assist component command TWGs with assessments of selected airfields. Advise HQ USEUCOM and USAFE of those airfields where assessments can or should be conducted by the Country Team.

(2) Coordinate with Host Nation officials for assessments of airfields.

## FOR OFFICIAL USE ONLY

(3) Coordinate with Host Nation officials and/or Country Team officials to facilitate augmented security for CAT B airfields.

(4) Coordinate with Country Team members such as the RSO to assist as appropriate.

(5) Notify HQ USEUCOM ECSM of any concerns or unresolved issues with component commands or Supporting CINCs.

### c. All Commands/Services/Agencies/Activities

(1) Each component command plays a key role in implementing an effective AT/FP program for the security of in-transit aircraft. In the USEUCOM AOR, each component command will conduct all-source threat analysis and vulnerability assessments to support risk assessments and the development of risk mitigation measures for ongoing and future air operations under the authority of that component.

(2) The responsible component command shall determine whether mitigating factors and recommendations are robust enough to counter the threat and present an acceptable risk for the air operation. Results of this process shall be presented in the form of a formal on-line risk assessment in the RAMP database that can be accessed through the USAFE/IN INTELINK-S homepage for RAMP 2.0 (<http://coldfusion.ramstein.af.smil.mil/RAMP/index.cfm>).

(3) Component commands shall assess current and potential threats affecting plans and operations of USEUCOM and other DoD forces in the USEUCOM AOR. Assessments shall include all-source intelligence to advise operators of the potential for military (air, air defense), information operations, terrorist, criminal, medical and foreign intelligence threats; local security arrangements; and operational limitations affecting USEUCOM AOR air operations.

(4) Component command TWGs, or functional equivalent, shall recommend mission "GO" or "NO GO" decisions and/or offer risk mitigation recommendations for both Security CAT "A" and CAT "B" airfields and air routes. Component commanders will establish an approval process for mission "GO" or "NO GO" decisions and mitigation recommendations. Approval authority must remain at the General/Flag Officer level. TWGs may selectively recommend additional measures at CAT "A" airfields for unique operations or during periods of heightened threat. Risk mitigation recommendations will be a coordinated product of all relevant agencies (usually operations, intelligence, military police/security forces, counterintelligence and medical). The number and types of measures proposed will be synchronized with mission requirements. Recommendations will be supplemented with the intelligence data providing the justification. In times of war or conflict, recommendations will be tailored to mission accomplishment—a "NO GO" recommendation may not be possible. Risk mitigation measures include, but are not limited to, the following:

**E-1-D-2**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

- Employ aircraft defensive systems (ADS)
- Vary arrival and departure times.
- Restrict airfield operations to daylight hours only.
- Restrict ground time.
- Enforce personal protection measures.
- Arm crewmembers.
- Provide Combat Air Patrols (CAP) to protect operating locations.
- Provide counter-battery capability to support operations at a forward location. (This is primarily considered only during combat operations.)
- Carry chemical gear. (This recommendation will be made if a location is in range of a country that possesses a lethal or incapacitating agent capability and is engaged in some level of hostilities with the United States.)
- Deploy Security Teams/Arrange for additional Host Nation Security/Contract local security (possibly through DAO/RSO).
- Remain on airfield.
- No Remain Overnight
  
- **Employ aircraft defensive systems (ADS):** Will be made regarding areas where there exists a significant or high antiaircraft threat, especially from antiaircraft artillery or man-portable, surface-to-air missiles (MANPADs). If aircraft that are not ADS-equipped must operate out of that location, other risk mitigation measures may be proposed.
  
- **No Remain Overnight (NO-RON):** This recommendation will cover locations where the local threats (Crime, Terrorism, Medical, Political/Military, and Foreign Intelligence Service) preclude personnel being billeted in the local area. If RON is a mission requirement, the TWG will prepare specific risk mitigation recommendations.
  
- **Location/Mission GO/NO GO:** A NO GO recommendation will be made only when no reasonable risk mitigation efforts can suppress the threat adequately to allow for the safe completion of the mission.
  
- **Secure Launch Country List:** USAFE maintains a list that identifies a country where the security situation is fluid and could deteriorate with little warning, creating such dangerous conditions that aircraft scheduled to fly there would be at serious risk. A country is added to the list if it meets at least one of these criteria: SIGNIFICANT or HIGH terrorist threat; chronic instability in the area of U.S. military operations; large US military presence or footprint in a country that may provide a lucrative target for anti-US elements.
  
- **Deployed Security Team:** Identifies airfields where security is inadequate and additional threats indicate a need for security personnel to provide dedicated aircraft security.

E-1-D-3

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

**(5)** Component commanders and Task Force commanders shall conduct airfield risk assessments IAW the guidance in Annex E, Appendix 1, and are responsible for RAMP database entries IAW with paragraph 5c(4), Annex E.

## FOR OFFICIAL USE ONLY

### TAB E (AIRFIELD RESPONSIBILITY MATRIX) TO APPENDIX 1 (SECURITY FOR IN-TRANSIT AIRCRAFT) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPORD 01-01

#### REFERENCES: See Basic Order

**GENERAL.** The following matrix lists the airfields and helipad/landing zones by component command in accordance with paragraph 3b(1)(a) of Annex E, and paragraph 4c of Annex E, Appendix 1. The listing is provided to assist each component command in scheduling required pre-deployment vulnerability assessments of airfields and accomplishing necessary coordination to de-conflict assessment schedules and eliminate redundancy.

1. This airfield listing and allocation of assessment responsibilities was developed by the USEUCOM executive agent for program management at HQ USAFE, and is current as of the date of this OPORD; however, it is recognized that this listing will continue to expand as new locations surface for exercises, Distinguished Visitor (DV) missions, and other additions to current component command operations. As a result, locations will be added and changes in responsibility may occur.
2. This matrix will be updated periodically via FRAGO issued by HQ USEUCOM. To view the most current airfield listing and responsibility matrix, refer to the airfield RAMP database or contact the HQ USAFE Threat Working Group (TWG).
3. As the USEUCOM executive agent for this program, HQ USAFE shall coordinate the further development of the Airfield Responsibility Matrix with USAREUR, USNAVEUR, MARFOREUR, SOCEUR and other appropriate commands. Proposed changes and updates to the listing shall be addressed to HQ USAFE. Concerns and/or issues regarding the allocation of responsibility should be referred to HQ USEUCOM ECSM for resolution.

## FOR OFFICIAL USE ONLY

USAFE Responsible Airfields		
Albania, Tirane	Germany, Memmingen	Latvia, Riga
Algeria, Algiers	Germany, Munchen	Liberia, Monrovia
Austria, Vienna	Germany, Nordholz	Lithuania, Vilnius
Belgium, Beauvechain	Germany, Norvenich	Luxembourg, Luxembourg
Belgium, Brussels	Germany, Ramstein	Macedonia, Skopje
Belgium, Chieveres	Germany, Rhein Main	Mali, Bamako
Belgium, Florennes	Germany, Spangdahlem	Montenegro, Podgorica
Belgium, Klien-Brogel	Germany, Stuttgart	Morocco, Marrakech
Belgium, Melsbroek	Germany, Weisbaden	Morocco, Rabat
Bosnia, Banja Luka	Ghana, Accra	Morocco, Saiss Fez
Bosnia, Mostar	Greece, Araxos	Morocco, Sidi Slimane
Bosnia, Sarajevo	Greece, Makedonia	Namibia, Grootfontein
Bosnia, Tuszla	Greece, Souda Bay	Namibia, Walvis Bay
Bulgaria, Sofia	Guinea, Conakry	Namibia, Windhoek
CAR, Bangui	Hungary, Balaton	Netherlands, Leewarden
Croatia, Durbrovnik	Hungary, Budapest	Netherlands, Maastircht
Croatia, Rijeka	Hungary, Taszar	Netherlands, Uden/Volkel
Croatia, Split	Hungary, Tokol	Netherlands, Valkenburg
Croatia, Zadar	Hungary, Veszprem	Netherlands, Hague
Croatia, Zargreb	Iceland, Keflavik	Niger, Niamey
Cyprus, Larnaca	Israel, Ben Gurion	Nigeria, Abuja
Cyprus, Akrotiri	Israel, Haifa	Nigeria, Lagos
Denmark, Vaerlose	Israel, Megiddo	Nigeria, Sokoto
Denmark, Aalborg	Israel, Nevatim	Norway, Bardafus
Denmark, Karup	Israel, Ramat David	Norway, Bodo
Denmark, Vojen/Skrydstrup	Israel, Rosh Pinna	Norway, Narvick
Estonia, Tallinn	Israel, Gaza	Norway, Orland
France, Cannes	Italy, Aviano	Norway, Oslo (ENFB)
France, Paris/Le Bourget	Italy, Brindisi	Norway, Oslo (ENGM)
Gambia, Banjul	Italy, Capodochino	Norway, Stavanger
Georgia, Tbilisi	Italy, Decimomannu	Portugal, Lajes
Germany, Berlin-Tegel	Italy, Falconara	Portugal, Montijo
Germany, Berlin-Templehof	Italy, Ghedi	Romania, Bucharest
Germany, Frankfurt (EDDF)	Italy, Gioia Del Colle	Romania, Craiova
Germany, Furstenfeldbruck	Italy, Pisa	Russia, Moscow
Germany, Geilenkirchen	Italy, Rome	Russia, Saratovo
Germany, Grafenwohr	Italy, Sigonella	Rwanda, Kigali
Germany, Hahn	Italy, Venezia Tessera	S Africa, Bloemfontein
Germany, Holzdorf	Italy, Vicenza	S Africa, Cape Town
Germany, Koln-Bonn (Mil)	Ivory Coast, Abidjan	S Africa, Durban
Germany, Laage	Kosovo, Pristina	S Africa, Hoedspruit
		S Africa, Johannesburg
		S Africa, Pretoria

**E-1-E-2**

**FOR OFFICIAL USE ONLY**



**FOR OFFICIAL USE ONLY**

USAFE Responsible Airfields (cont'd)		
S Africa, Waterkloof	Turkey, Adana	UK, Farnborough
Senegal, Dakar	Turkey, Adnan Menderes	UK, Kinlos
Senegal, Tambacounda	Turkey, Akhisar	UK, Lakenheath
Sierra Leone, Freetown	Turkey, Ankara (LTAD)	UK, Leuchars
Slovakia, Bratislava	Turkey, Ankara (LTAE)	UK, London (EGLL)
Slovakia, Kosice	Turkey, Antalya	UK, London (EGSS)
Slovakia, Malacky	Turkey, Balikesir	UK, Lossiemouth
Slovakia, Sliac	Turkey, Bandirma	UK, Lyneham
Slovenia, Ljubljana	Turkey, Bayuk Cigli	UK, Mildenhall
Spain, Barcelona	Turkey, Corlu	UK, Newquay
Spain, Madrid	Turkey, Diyarbakir	UK, Northholt
Spain, Menorca	Turkey, Eskisehir	UK, Halifax
Spain, Sevilla	Turkey, Incirlik	UK, Yeovil
Spain, Zaragoza	Turkey, Ismir (LTBK)	Ukraine, Kharkov
Switzerland, Geneva	Turkey, Ismir (LTFB)	Ukraine, Kiev
Switzerland, Zurich	Turkey, Ismit	Ukraine, Lvov
Syria, Damascus (OSDI)	Turkey, Istanbul	Ukraine, Odessa
Syria, Damascus (OSMZ)	Uganda, Entebe	Ukraine, Sevastopol
Tunisia, Carthage	UK, Biggin Hill	Yugoslavia, Belgrade
Tunisia, Sidi Ahmed	UK, Brize Norton	Zimbabwe, Harare Int
S Africa, Upington	UK, Cottesmore	Zimbabwe, Victoria Falls
	UK, Fairford	

NAVEUR Responsible Airfields		
Belgium, Oostende	Greece, Elefsis	Malta, Malta
Bulgaria, Varna	Greece, Eletherios Venizelos	Portugal, Beja
Croatia, Pula	Greece, Ionnis Kapodistrias	Spain, Ibiza
Croatia, Udbina	Greece, Larisa	Spain, Malaga
France, Cote D Azur	Italy, Alghero	Spain, Murcia San Javier
France, Le Palyvestre	Italy, Bari	Spain, Palma
France, Marseilles	Italy, Bologna	Spain, Reus
France, Merignac/Bordeaux	Italy, Casale	Spain, Rota
France, Solenzara	Italy, Grottaglie/Marlotta	Spain, Valencia
France, Hyres	Italy, Palese Macchie	Tunisia, Bizerete
Gabon, Gibraltar	Italy, Rimini	Turkey, Dalaman/Mugla
Germany, Bremen	Italy, Ronchie Dei Legionari	UK, Bournemouth
Germany, Bruggen	Italy, Trapani	UK, Edinburgh
Greece, Athinai	Malta, Luqa	UK, St Magwan

## FOR OFFICIAL USE ONLY

USAREUR Responsible Airfields		
Armenia, Zvartnots	Germany, Fritzlar	Germany, Niederstetten
Austria, Graz	Germany, Giebelstadt AAF	Germany, Nuebrucke HP
Austria, Linz	Germany, Giessen HP	Germany, Nurnberg
Belgium, Melsbroek	Germany, Gutersloh	Germany, Oberauerbach HP
Bulgaria, Burgas	Germany, Hamburg	Germany, Oberpfaffenhofen
Finland, Ivalo	Germany, Hammond Barracks HP	Germany, Paderborn Lippstadt
France, Carpiquet	Germany, Hanau AAF	Germany, Panzar Kaserne HP
France, Dijon	Germany, Hannover	Germany, Patch Barracks HP
Germany Bonn Hardthohe HP	Germany, Heidelberg AAF	Germany, Oberammergau HP
Germany, Aachen Merzbruck	Germany, Heringsdorf	Germany, Ray Barracks HP
Germany, Augsburg	Germany, Hof Plauen	Germany, Rhein Bentlage
Germany, Bad Aibling HP	Germany, Hohenfels AAF	Germany, Rhein Ord Barracks HP
Germany, Bad Kissingen	Germany, Hohenfels Hosp Pad	Germany, Rheingalen HP
Germany, Bad Kreuznach AHP	Germany, Hohenfels Main AHP	Germany, Robinson Barracks HP
Germany, Baden Baden	Germany, Hopsten	Germany, Roth
Germany, Badenhausen AHP	Germany, Illesheim AHP	Germany, Saarbrucken
Germany, Bamberg AAF	Germany, Ingolstadt Manching	Germany, Schleswig
Germany, Baumholder AAF	Germany, Itzehoe Hungruer Wolf	Germany, Schweinfurt AHP
Germany, Baumholder Hosp Pad	Germany, Jaeger Kaserne HP	Germany, Sheridan Kaserne HP
Germany, Bayreuth	Germany, Jever	Germany, Sonthofen HP
Germany, Berchtesgaden	Germany, Kaiserslautern Depot AHP	Germany, Taylor Barracks HP
Germany, Berlin-Schonefeld	Germany, Karlsruhe	Germany, Tomplins Barracks HP
Germany, Boeblingen HP	Germany, Kelly Barracks HP	Germany, Vilseck AAF
Germany, Bremerhaven	Germany, Kiel-Holtenau HP	Germany, Vilseck Main AHP
Germany, Buchel	Germany, Koblenz Winnigen	Germany, Volgelweh HP
Germany, Buckeburg	Germany, Lahr	Germany, Wiley Barracks HP
Germany, Buingen AHP	Germany, Landsberg Lech	Germany, Willingen Hotel HP
Germany, Celle	Germany, Landstuhl AHP	Germany, Wittmundhafen
Germany, Chiemsee HP	Germany, Landstuhl Hosp Pad	Germany, Wunstorf
Germany, Coleman AAF	Germany, Larson Barracks HP	Greece, Kerkira
Germany, Cottbus	Germany, Laupheim	Guernsey, Guernsey
Germany, Dexheim HP	Germany, Lechfeld	Italy, Barri
Germany, Diepholz	Germany, Lee Barracks HP	Italy, Lecee
Germany, Dresden	Germany, Mainz-Finthen	Moldova, Chisinau
Germany, Dusseldorf	Germany, Marshall Center HP	Netherlands, Brunssum HP
Germany, Eggebek	Germany, Mendig	Poland, Babimost
Germany, Erding	Germany, Monchengladbach	Poland, Szprotawa
Germany, Fassberg	Germany, Neubrandenburg	Poland, Warsaw
Germany, Freedom Field HP	Germany, Neuburg	Poland, Zagan
Germany, Freiburg		

**E-1-E-4**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

SOCEUR Responsible Airfields		
Denmark, Sonderburg	Lithuania, Palanga	Poland, Krakow
France, Agen	Mali, Gao	Romania, Bacau
France, Anglet	Mali, Mopti	Romania, Mihail Koglniceanu
France, Istres	Mali, Tobouctou	Slovenia, Cerklje
France, Mont De Marsan	Morocco, Ben Guerir	Spain, Almeria
France, Tarbes	Morocco, Kenitra	Spain, Granada
France, Toulouse	Morocco, Meknes	Spain, Moron
Greece, Skyros	Netherlands, Dekooy	UK, Leeming
Greece, Tanagra	Netherlands, Soesterberg	UK, Marihanish
Greece, Tmpaki	Norway, Alta	UK, Prestwick
Hungary, Kecskemet	Norway, Andoya	UK, Valley
Hungary, Szolnok	Norway, Evenes	UK, West Freugh

MARFOREUR Responsible Airfields		
Azerbaijan, Baku	Cape Verde, Amilcar Cabral	Norway, Vaernes

USAFE Responsible Airfields (Used by TRANSCOM, not requested by a EUCOM Component)		
Benin, Cotonou	Finland, Tampere Pierkala	Poland, Strachowice
Botswana, Gaborone	Gabon, Liberville	South Africa, Capetwon
Burundi, Bujumbura	Ireland, Dublin	South Africa, Hoedspruit
Cameron, Doulal	Ireland, Shannon	South Africa, Johanesburg
Cameron, Garoua	Israel, Ovda Airport	South Africa, Waterloof
Cameron, Yaounde	Mauritania, Nouakchott	Sweden, Gotheburg
Chad, N'Djamemat	Moldova, Chisinau	Sweden, Stockholm
Congo, Goma Int	Mozambique, Beira	Syria, Latakia
Congo, Kinshasa	Mozambique, Mauto	Tanzania, Dar Es-Salaam
Czech Repub, Ruzyne	Namibia, Hosea	Tanzania, Kilamanjaro
Czech Repub, Turany	Nigeria, Ibadan	Turkey, Grand Turk
Eritrea, Asmara	Nigeria, Kano	UK, Birmingham
Finland, Helsinki Cantaa	Nigeria, Niamey	UK, Waddington
		Zambia, Lusaka

USAFE Responsible Airfield (Used by JFCOM, not requested by a EUCOM Component)
France, Lann Bihoue

CENTCOM AOR Airfields		
Djibouti, Djibouti	Kazakhstan, Almaty	Saudi Arabia, King Khaldi
Egypt, Alexandria	Kazakhstan, Astana	Saudi Arabia, Prince Sultan
Egypt, Cairo West	Kenya, Mombasa	Saudi Arabia, Riyadh
Egypt, Hurghada	Kenya, Nairobi	UAE, Dubai
Egypt, Luxor	Krygyzstan, Bishek	UAE, Fujairah Int'l
Egypt, Sharm El Sheikh	Kuwait, Kuwait	Uzbekistan, Tashkent
Jordan, Aqaba	Saudi Arabia, Dhahran	Yemen, Aden

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**E-1-E-6  
FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### TAB F (AIRFIELD ASSESSMENT CHECKLIST) TO APPENDIX 1 (SECURITY FOR IN-TRANSIT AIRCRAFT) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPOD 01-01

**REFERENCES:** See Basic Order

**GENERAL INSTRUCTIONS.** When conducting an airfield survey, the questions in the Sample Airfield Assessment Checklist, below, should be answered and included in the survey report.

1. The paragraph format and numbering in the sample below should be adhered to. Those items identified by an asterisk (\*) are considered critical information and are mandatory inputs for all survey reports.
2. 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 component command for inclusion in the airfield Risk Assessment Management Program (RAMP) database.
3. When on-site multi-disciplined assessment teams are not required for Security CAT "B" airfields, the checklist and survey report may be completed by aircrew members, security personnel accompanying the aircraft, or the U.S. Embassy Defense Attache (DATT) or Regional Security Officer (RSO). Individual(s) conducting the survey/assessment will forward the report electronically to the responsible component command.
4. For Security CAT "A" airfield assessments, asterisked (\*) items and other items determined to be critical by the responsible component command will be completed by aircrew members, RSO, DAO, or others as deemed appropriate.
5. The Airfield 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/FP Plan or specific mission, the classification of the document in its entirety will be CONFIDENTIAL, although extracted data may remain FOUO/SBU.

# FOR OFFICIAL USE ONLY

## SAMPLE AIRFIELD 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

1.1. \*Is the airfield perimeter completely fenced or walled (type, height, condition, gaps, holes, etc.)?

1.2. \*Is the flight line/ramp fenced? Describe (type, height, condition, gaps, holes, etc.).

1.3. Are there clear zones on each side of the fence/wall? If so, describe the clear zone to include width and nature.

1.4. Is the airfield perimeter or flight line area posted "No Trespassing" or "No Admittance"?

#### 1.5. Other Physical Barriers

1.5.1. List different types, locations and numbers of barriers used on the perimeter, and on/near the flight line/ramp.

1.5.2. Is the airfield or aircraft parking areas under surveillance, e.g., Closed Circuit Television (CCTV)?

#### 2. Security Force Level

2.1. \*How many guards are typically on duty during the day and night?

2.2. \*Are these guards host nation military units? Police or security police? Contract guards?

2.3. To what extent can the existing security force be augmented by in-place or nearby personnel? How long can the augmented posture be maintained?

**E-1-F-2**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

2.4. What are shift durations and shift change procedures/times?

2.5. What local customs or other factors might result in degraded security, e.g., national holidays, traditional daily rest periods, etc.?

### 3. Security Personnel

3.1. Are personnel well trained and professional? Does this vary by position? Are the supervisory personnel better trained or more motivated?

3.2. 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.?

3.2.1. Is the reliability of the security guard force in question?

3.3. \*What is the predominant language or dialect spoken by security forces? Indicate what percentage of the security force speaks English (if applicable)?

3.4. \*To what degree are they willing to work with U.S. and/or Allied personnel?

3.5. \*Are security forces willing and able to provide increased security for U.S. and/or Allied missions?

3.5.1. \*If so, how are such arrangements made? Through U.S. Defense Representative (USDR)?

### 4. Security Patrols

4.1. \*Is the perimeter and/or flight line controlled by armed guards?

4.2. \*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?

4.3. \*Are patrols made on foot, animals, or vehicles?

4.4. How many people are on each patrol?

4.5. Do patrols use working dogs?

### 5. Security Equipment

5.1. \*Are guards armed?

## **FOR OFFICIAL USE ONLY**

5.1.1. \*What types of weapons are carried by guards?

5.1.2. \*Do guards have adequate ammunition levels? What is the basic load?

5.2. What additional weapons are available (what weapons can be used, if needed; what weapons are used on vehicles, at entry points, guard towers, etc.)?

5.3. \*What forms of communications gear do the security personnel use?

5.4. Do the security personnel have protective masks available?

5.5. Do the security personnel wear body armor/bullet resistant vests/helmets?

5.6. Are explosives detector dog teams available and employed?

### **6. Watch Towers/Fixed Guard Positions**

6.1. How many ground level guard shacks, elevated towers, fixed fighting positions and/or bunkers, etc., are there? List by location and give description.

6.2. How many guards are there at each location?

### **7. Quick Reaction/Counterterrorist Units**

7.1. \*Does such a force exist?

7.2. \*Is it on or near the airfield?

7.3. \*What is the reaction time of this force?

7.4. \*How large a force is it?

7.5. What are the command and control arrangements? To what degree is responsibility delegated in crisis situations?

7.6. How is the force trained and equipped?

7.7. Does it have higher morale than the regular guard force?

7.8. Has it successfully conducted operations in the past?

### **8. Entry Control Points (ECP)**

8.1. \*Is entry to the installation and flight line/ramp controlled?



## FOR OFFICIAL USE ONLY

**8.2.** \*How many ECPs are there on the perimeter and flight line/ramp areas? Give the location and description of each ECP.

**8.3.** \*Are gates locked if unmanned?

**8.3.1.** Describe the type of gate (and locking device, if applicable).

**8.4.** \*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.

**8.4.1.** Are interior ramp access doors locked or have controlled entry when open?

**8.5.** Are X-Ray machines and/or metal detectors used at any of the entry points?

**8.6.** If entry is controlled, what form of personal identification is required for individuals and vehicles? Distinguish between airfield and flight line/ramp procedures.

**8.7.** \*Are private vehicles allowed on the flight line/ramp? If so, what method of registration (or pass system) is required?

**8.8.** Are all persons in a vehicle required to show identification?

**8.9.** What are the visitor control procedures, e.g., procedures for visitor approval, and identification of same?

**8.10.** What are visitor escort procedures?

**8.11.** To what degree are vehicles, personnel, and their possessions searched?

**8.12.** \*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**

**9.1.** \*Is the entire boundary of the airfield, flight line, and/or aircraft parking ramp lighted at night?

**9.2.** Are additional fixed spotlights located at watchtowers and/or entry points?

**9.3.** Are mobile mounted/towable spotlights available?

### **10. Parking**

**10.1.** \*Are DoD aircraft parked in special locations (isolated from other aircraft)? \*If so, are additional guards posted?

## FOR OFFICIAL USE ONLY

10.1.1. What is the distance from buildings, perimeter fence and non-DoD aircraft?

10.1.2. Are barriers available for aircraft parking locations?

10.2. Is the area clearly marked as a restricted and/or controlled area?

10.3. \*Are DoD personnel authorized to have weapons on the flight line/ramp?

10.4. Are Service approved weapons storage facilities available to transiting crews?

**11. Billeting. Complete the following when it anticipated that DoD aircraft may be required to remain over night at foreign airfields.**

11.1. Does the American Embassy (Amembassy) provide billeting in its compound? If billeting is unavailable at the compound, does Amembassy (DATF or RSO) maintain a list of hotels that meet minimum security requirements?

11.2. If the Amembassy maintains a list of recommended hotels, request the following information on each, if available:

11.2.1. Basic description (design, height, interior/exterior entrances, number of rooms).

11.2.2. General layout (parking areas, fencing, lighting, proximity to highways and/or major roads).

11.2.3. Number of elevators/stairways (internal/external), building entrances/exits, security features for rooms, vehicle entrances/exits.

11.2.4. Are DoD personnel billeted in the same areas of the hotel, or are they separated? Are there telephones in the rooms?

11.2.5. How is the crew transported to and from the hotel?

11.2.6. Are metal detectors/x-ray machines used at hotel entrances?

11.2.7. Is there a 24 hour front desk operation?

11.2.8. Is there a 24 hour armed hotel guard force?

11.2.9. Are security forces available to escort crews transiting to/from the airfield?

**12. Off Installation Route Security. Complete the following when it anticipated that DoD aircraft may be required to remain over night at foreign airfields.**

12.1. What is the distance from airfield to hotel?

## FOR OFFICIAL USE ONLY

**12.2.** How many different routes are there from airport to hotel?

**12.2.1.** Provide a description of each route.

**12.2.2.** 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.

**12.2.3.** Identify number of lanes each way.

**12.2.4.** Identify one-way streets.

**12.2.5.** Identify the number and location of safe houses (i.e., police stations) along each route.

**12.3.** Do host nation security authorities regularly patrol these routes?

**12.3.1.** Are host nation security escorts available?

**12.4.** Has there been any reported incidents of surveillance in the past 12 months?

### **13. Physical Location**

**13.1.** What natural and/or manmade obstacles are in the vicinity of the airfield, e.g., power lines, tall buildings, etc.?

**13.2.** Are there areas surrounding flight line parking area that could be used by hostile elements to covertly observe airport operations and to launch attacks?

**13.3.** How suitable is the surrounding terrain and vegetation for staging a stand-off attack? Does this vary seasonally?

**13.4.** What is the proximity of vehicle parking and public access areas to the aircraft parking area?

**13.5.** 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 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.)**

**E-1-F-7**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### 16. Description of facility/service surveyed:

### 17. Individual(s) interviewed:

17.1. Name, Rank/Grade, Organization, Phone Number

### 18. Service Vendor Control

18.1. For each Service Provider, determine:

18.1.1. Contractor Name (if different from Interviewee listed above):

18.1.2. Supervisor's Name:

18.1.3. How long has the service been supplied?

18.1.4. Is there an up-to-date list of names and addresses of all contractor employees?

18.1.4.1. Are background checks accomplished on the contractor and subcontractor employees? Is a favorable background check required for employment?

18.1.4.1.1. Are the background checks available for review?

18.1.5. Do vehicles of contractor employees, which enter the facility, have an identifying decal (or pass system)?

18.1.6. Are the vehicles of contractor employees inspected?

18.1.6.1. How Often?

18.1.7. Is there an identification system for contractor employees?

18.1.7.1. Are picture identification badges used?

18.2. How are vendors controlled on the flight line/ramp?

18.3. Is a single egress/ingress control point to the flight line/ramp used for all vendors, repairmen, etc.?

### 19. Vendor Vehicle/Equipment Security

19.1. Are the vehicles/equipment marked with vendor logo(s)?

19.2. Are key control procedures used by the vendor?

## **FOR OFFICIAL USE ONLY**

**19.2.1** Who is responsible for issuance of keys?

**19.2.2.** Are all keys accounted for?

**19.2.3.** Is issuance of keys recorded?

**19.2.3.1.** Are keys signed for?

**19.2.3.2.** Is report kept up to date?

**19.2.4.** Who has access to Master keys? (Name, Position, Number of people)

**19.2.5.** Are keys removed from vehicles when not in use, at night and on weekends?

**19.2.6.** Is there a procedure for return of keys when an employee is terminated or transferred?

**19.2.7.** Physical vehicle/equipment control

**19.2.7.1.** 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?

**19.2.7.1.1.** Is the area in view of assigned personnel during normal working hours?

### **20. Vendor Service Capability**

**20.1.** For each service provider, determine the following:

**20.1.1.** On average, how many vehicles/pieces of equipment are in service?

**20.1.2.** What is the average response time?

### **SECTION III: HOST NATION MEDICAL FACILITIES**

#### **21. Hospital Information**

**21.1.** Location, phone numbers, POCs

**21.2.** What is the distance from the airfield (time by air/ground)?

**21.3.** What type of hospital (Military/Civilian)?

**21.4.** Does Support Agreement or MOU exist with the hospital?

#### **22. Services Available**

## **FOR OFFICIAL USE ONLY**

- 22.1.** What is the inpatient capability and number of beds?
- 22.2.** How many ICU beds are there?
- 22.3.** What is the Emergency Service Capability?
- 22.3.1.** What resources are available?
- 22.3.2.** What is the size and experience of the staff?
- 22.4.** Is there an Emergency Medical Response capability?
- 22.5.** Is there a HAZMAT/NBC Response capability?
- 22.6.** Is equipment such as X-ray, CT Scan, MRI available (condition of equipment, availability of support equipment, quality of images)?
- 22.7.** Are Lab facilities available (capabilities, condition of facilities)?
- 22.8.** How many ambulances are available? What is their capacity?
- 22.9.** Is there a Blood Banks? How many Units are available?
- 22.10.** Is there a Burn Center?
- 22.11.** Are there Decontamination/Isolation Areas?
- 23. Medical Evacuation**
- 23.1.** Are there existing air strips capable of supporting aircraft used for evacuation?
- 23.2.** Does a rotary wing evacuation pad exist?
- 23.3.** 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.
- 23.4.** Is liquid or gaseous oxygen available?
- 23.5.** 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.
- 23.6.** 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**

## FOR OFFICIAL USE ONLY

- 24.1. What are the lodging provisions for aircrews? (See items 11-13, above)
- 24.2. Is there a sanitary Linen/Room/Environment?
- 24.3. Is the water and plumbing acceptable (sink/toilet)?
- 24.4. If malaria is of concern, are there screens on windows or functioning air conditioning?
- 24.5. What are the arrangements for feeding aircrews? (e.g., distance from airfield, same as lodging, etc.)
- 24.6. Have off-base food facilities been inspected by host nation civilian or military Preventive Medicine personnel? List POC and telephone numbers.
  - 24.6.1. Are inspection reports available? Obtain copies.
- 24.7. What is the source of meat products?
- 24.8. What is the source of frozen products?
- 24.9. What is the source of dry goods?
- 24.10. What is the source of fresh products?
- 24.11. What is the source of dairy products?
- 24.12. Are adequate food storage facilities available for dry items?
- 24.13. Are adequate food storage facilities available for refrigerated/frozen items?
- 24.14. Are food-handlers (cooks and servers) aware of HACCP-type guidelines?
- 24.15. Does facility appear sanitary (absence of rodents, clean food contact surfaces, etc.)?
- 24.16. Are approved food sources, including bottled water, available?
- 24.17. Are local sources for bottled water products available? List what to avoid if any.

### 25. Public Water System

- 25.1. Does a public water system exist?
- 25.2. If yes, is it owned/operated by host nation military or civilian authorities? (If possible, obtain POC and telephone numbers.)

**E-1-F-11**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

**25.3.** What is the source of water, e.g., groundwater, surface water or groundwater under the influence of surface water?

**25.4.** 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.

**25.5.** Is there an active drinking water surveillance program from the host nation?

**25.6.** What is the form of treatment, disinfection, water quality sampling (collection, analysis, etc.)?

**25.7.** Based on host nation laws and regulations, what parameters are analyzed and at what frequencies?

### **26. Environmental/Industrial**

**26.1.** 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)?

**26.2.** How is disease transmission affected by the environment (vectors, flora, fauna, etc. Note source of information, e.g., observed vs. documented)?

**26.3.** What pollution exists (type, source, concerns, etc.)?

**26.4.** Are roads in good repair, streetlights, pedestrians, sidewalks, curbs, etc.?

**26.5.** Does environmental pollution appear to be a potential problem?

**26.6.** If yes, would it appear to be a threat to DoD personnel?

**26.7.** Do potential environmental/pollution hazards exist and in what form (nuclear power plant, fuel storage, chemical plants, agricultural spraying)?

**26.8.** Do Hazardous Material/Hazardous Waste (HM/HW) storage, handling, disposal practices exist?

**26.8.1.** If yes, would they appear to be a threat to DoD personnel?

**26.8.2.** If yes, supply additional information (type hazard, description, specific location, etc.).

**26.8.3.** Does the site (airfield and billeting) have the capability to respond to HM/HW release to the environment, e.g., chemical spills?

**E-1-F-12**

**FOR OFFICIAL USE ONLY**



# FOR OFFICIAL USE ONLY

## SECTION IV: HOST NATION FIRE DEPARTMENT

### 27. Fire Department general information

27.1. Does the airfield have a fire department?

27.2. Is the fire department a 24 hour operation?

27.2.1. If not, what are the operating hours?

27.3. Is the fire department located near the flight line? Do they have quick access to the flight line?

27.4. What equipment does the fire department have?

27.4.1. Is equipment operational?

27.5. Are the fire department personnel trained?

27.6. How do DoD personnel request fire department response?

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**E-1-F-14  
FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### APPENDIX 2 (SECURITY FOR IN-TRANSIT SHIPS) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPORD 01-01

#### REFERENCES: See Basic Order

- 1. PURPOSE.** To provide transient ships and accompanying personnel adequate security within the USEUCOM area of responsibility (AOR).
- 2. APPLICABILITY.** This Annex applies to all DoD or DoD chartered elements, ships and accompanying personnel operating in the USEUCOM AOR under the force protection responsibility of USCINCEUR. The following criteria outline force protection responsibilities of USCINCEUR and subordinate commanders:
  - a.** U.S. Naval vessels, Naval Fleet Auxiliary Vessels, MSC Vessels, and Combat Logistics Forces OPCON to USCINCEUR.
  - b.** U.S. Naval vessels, Naval Fleet Auxiliary Vessels, MSC Vessels, and Combat Logistics Forces TACON to USCINCEUR for force protection. An example of this category would be a submarine from SUBLANT during a port visit within the USEUCOM AOR.
  - c.** USCINCEUR and subordinate commanders exercise no force protection authority or responsibility for commercial vessels chartered by DoD, unless specifically provided for in the contract. When such vessels are carrying vital DoD material or DoD personnel (supercargo), commanders shall request threat assessments from supporting intelligence organizations and conduct a threat analysis/risk assessment to determine port security requirements. Commanders shall engage with the host nation and U.S. country team (as necessary) to ensure host nation and/or U.S. security measures are commensurate with the threat.
- 3. POLICY.** It is the policy of USCINCEUR to deter terrorism through the use of all reasonable means. While reducing the risk to USEUCOM resources from acts of terrorism is a command responsibility, each person in the USEUCOM AOR must exercise proper caution and prudent judgment to reduce their own exposure. Each USEUCOM activity (component command forces, DRUs) must establish guidelines of this order tailored to mission and local conditions.
- 4. PORT VISIT REQUIREMENTS**
  - a.** Components must be able to maintain continuous contact with transiting ships. Components will identify shortfalls in en route communications capabilities and will take steps to aggressively pursue the ability to contact ships, en route, anywhere in the USEUCOM AOR. Inability to satisfy this requirement will be reflected in executive/operations orders and considered during mission planning

## FOR OFFICIAL USE ONLY

and approval, but does not require submission of a waiver request to HQ USEUCOM.

b. Component Commanders and Task Force commanders will coordinate the conduct of port security/vulnerability assessments.

### 5. TRANSIENT OPERATIONS

a. Antiterrorism/Force Protection (AT/FP) planning must be conducted for each port visit including brief stops that require mooring, anchoring or operating in confined locations. AT/FP planning also is required for transiting restricted straits, canals and waterways. As a minimum, Port Visit AT/FP planning includes:

**(1) Assessments.** Threat and Port Vulnerability Assessments are key elements in the planning process and provide commanders a foundation for preparing their Inport Security Plans (ISP). NCIS provides port specific and strait transit threat assessments for every unit 7-10 days in advance. Task Force Commanders are addressees on messages containing USEUCOM Joint Analysis Center (JAC) Port assessments and/or country assessments. JAC assessments are updated approximately once per quarter or as circumstances require. Port Vulnerability Assessments (PVA) for a number of ports in the Mediterranean are available for ships' use in port visit planning. Threat and Vulnerability information is available on the SIPRNet at the COMSIXTHFLT Force Protection Homepage, <http://www.c6f.navy.smil.mil/>.

**(2) Inport Security Plans (ISP).** Ships will develop ISP's, which should include all measures in Tab A and Tab D, applicable to the current Force Protection Condition unless clearly not necessary (e.g., pier security measures for a ship at anchor). They should focus on employing non-lethal means first (barriers, verbal warnings, fire hoses, etc.), with lethal defense considered a last resort. Measures implemented onboard the ship may be employed at the commanding officer's discretion. Off-ship measures require host nation coordination and cooperation for approval, and are addressed in the LOGREQ Security Supplement. Specific AT/FP measures that fall into this category are those from a higher Force Protection Condition that occur off ship and/or require host nation support. See Tab A of this Appendix for an example of an ISP.

**(3) AT/FP LOGREQ Supplement.** While in Force Protection Condition BRAVO or higher, ships are to request support via separate LOGREQ. This procedure enhances AT/FP and ensures host nation support is coordinated through a single U.S. representative, usually the DAO. See Tab B of this Appendix for an example of a LOGREQ Supplement message.

**(4) Water Borne Security.** Each ISP should include measures to establish clear lines of demarcation (e.g., posted warnings, booms, or buoys) to

## FOR OFFICIAL USE ONLY

create standoff and to define protective concentric zones of defense around the ship. In situations where the host nation 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) Assessment zone.** Detect, localize, track, classify, inspect, identify and “tag” intruders as authorized, unauthorized, or unknown.

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

**(c) 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).

### ACKNOWLEDGE

**JOSEPH W. RALSTON**  
**General, USAF**

### TABS:

- A. Example of Inport Security Plan
- B. Example of LOGREQ Security Supplement
- C. Example of Inport Security Plan Approval
- D. Security Assessment Survey Form and Checklist for Non-U.S. Ports

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**E-2-4**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### TAB A (EXAMPLE OF INPORT SECURITY PLAN) TO APPENDIX 2 (SECURITY FOR IN-TRANSIT SHIPS) TO ANNEX E (SECURITY OF IN- TRANSIT FORCES) TO USCINCEUR AT/FP OPO RD 01-01

**GENERAL.** The following example is provided to illustrate the format and typical content of an Inport Security Plan (ISP). This example is not all inclusive.

1. Care must be taken in each case to ensure that Antiterrorism/Force Protection (AT/FP) measures and other planning factors are tailored to the local situation and existing threat.
2. Although the example is written as a classified message since an actual ISP would normally be classified at CONFIDENTIAL, none of the information in this example is classified.

#### Example of Inport Security Plan

FM USS NEVERSAIL

TO CTF

INFO COMSCEUR NAPLES IT//N3//  
COMSIXTHFLT  
CINCUSNAVEUR LONDON UK//N3/N4//  
COMSC WASHINGTON DC//PM1/N3//  
COMSCLANT NORFOLK VA//N3//  
MSC NFAF EAST NORFOLK VA//PM1E//  
NAVCRIMINVSERVFO EUR NAPLES IT//JJJ//  
NAVCRIMINVSERVRA (location)//JJJ//  
HQ USEUCOM VAIHINGEN GE//ETCC/ECJ2/ECSM//  
JAC MOLESWORTH RAF MOLESWORTH UK//DOA//

C O N F I D E N T I A L //N00000//

MSGID/GENADMIN/USS NEVERSAIL//

SUBJ/INPORT SECURITY PLAN FOR (LOCATION)(U)//

REF/A/MSG/CINCUSNAVEUR/INPORT AT/FP GUIDANCE/DTG//

REF/B/DOC/USCINCEUR OPO RD 01-01/DTG//

REF/B/DOC/COMSCINST5530.3B/DTG//

NARR/(U) REFS A AND B ESTABLISH AT/FP REQUIREMENTS FOR USEUCOM AOR TO INCLUDE GUIDELINES FOR INPORT SECURITY PLANS. REF C IS COMSC INSTRUCTION FOR MSC SHIP PHYSICAL SECURITY.//

RMKS/1. (U) IAW REFTELS, THE FOLLOWING INPORT SECURITY PLAN IS SUBMITTED FOR PVST XXXXX (DATES OF VISIT). THIS PLAN IS TAILORED TO FORCE PROTECTION CONDITION XXXXX, THREAT LEVEL XXXXX FOR XXXXX, AND COMPLIES WITH REFTELS.

**E-2-A-1**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

- A. (C) ALL CREW MEMBERS HAVE RECEIVED LEVEL 1 ANTI-TERRORISM TRAINING. THE FIRST OFFICER HAS COMPLETED FORCE PROTECTION OFFICER TRAINING. SET TRAINING WAS LAST CONDUCTED 09/06/2000. 10 CREW MEMBERS ARE CURRENTLY SMALL ARMS QUALIFIED. ALL HANDS HAVE BEEN BRIEFED IN THE MEANING OF FORCE PROTECTION CONDITION BRAVO AND MEASURES FOR TRANSITIONING TO FORCE PROTECTION CONDITION CHARLIE AND DELTA AS REQUIRED IN REF B.
- B. (C) MAIN PROPULSION WILL REMAIN AT A LEVEL OF READINESS TO PERMIT GETTING UNDERWAY ON SHORT NOTICE. SUFFICIENT PERSONNEL WILL REMAIN ONBOARD TO PROVIDE PHYSICAL SECURITY AND EMERGENCY GETTING UNDERWAY.
- C. (C) IN-PORT DECK WATCH WILL CONSIST OF ONE WATCH OFFICER, ONE QUARTERDECK WATCHSTANDER, ONE OFFSHORE DECK WATCH, ONE ROVING SECURITY WATCH MAKING DETEX ROUNDS BETWEEN THE HOURS OF 18-06. ALL WATCH PERSONNEL WILL BE EQUIPPED WITH WHISTLE AND RADIO.
- D. (C) CARS, TRUCKS, GARBAGE DUMPSTERS, CARGO, AND OBJECTS ON THE PIER WILL BE INSPECTED AND TREATED WITH SUSPICION. NO VEHICLES WILL BE ALLOWED NEAR THE SHIP OR GANGWAY. ALL VEHICLE TRAFFIC WILL BE INSPECTED AND CHECKED AGAINST AN AUTHORIZED ACCESS LISTING PRIOR TO ACCESS TO THE PIER.
- E. (C) THE GANGWAY WATCH WILL INSPECT ALL BAGS AND CHECK ALL ID'S PRIOR TO BEING ALLOWED ONBOARD. NO UNOFFICIAL VISITORS WILL BE ALLOWED ONBOARD. ALL VISITORS WILL BE LOGGED ONBOARD AND ISSUED A VISITOR BADGE WITH ESCORT AS REQUIRED.
- F. (C) GARBAGE BOAT WILL BE LOADED VIA PIER VICE ALONGSIDE.

2. (C) FORCE PROTECTION CONDITION ALPHA/BRAVO MEASURES THAT VESSEL CANNOT COMPLY WITH: MEASURE 25, CANNOT KEEP UNAUTHORIZED CRAFT AWAY FROM SHIP; AND MEASURE 18, PIER SENTRY PROVIDED BY LOCAL HOST NATION FORCES.

3. (U) THE FOLLOWING SOURCES HAVE BEEN USED TO OBTAIN INFORMATION IN DEVELOPING THIS INPORT SECURITY PLAN: NCIS HOMEPAGE HAS BEEN QUERIED FOR LATEST SECURITY INFORMATION REGARDING XXXXX. **(NOTE: List all references checked.)//**

DECL/OADR//

BT  
NNNN



## FOR OFFICIAL USE ONLY

### TAB B (EXAMPLE OF LOGREQ SECURITY SUPPLEMENT) TO APPENDIX 2 (SECURITY FOR IN-TRANSIT SHIPS) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPORD 01-01

**GENERAL.** The following example is provided to illustrate the format and typical content of a LOGREQ Security Supplement. This example is not all inclusive.

1. Care must be taken in each case to ensure that Antiterrorism/Force Protection (AT/FP) measures and other planning factors are tailored to the local situation and existing threat.
2. Since one of the primary purposes of this action is to maximize AT/FP support from host nation authorities, care must be taken when listing those measures requiring host nation assistance and coordination. While the overall classification of the message normally would be CONFIDENTIAL based upon compilation rules, individual paragraphs containing specific measures requiring release to host nation authorities, to include non-military personnel and agencies, would be FOR OFFICIAL USE ONLY.
3. Although the example, below, is written as a classified message since an actual LOGREQ Security Supplement message would normally be classified at CONFIDENTIAL, none of the information in this example is classified.

#### Example of LOGREQ Security Supplement

FM USS NEVERSAIL

TO USDAO XXXXXXXXXXXX  
INFO CINCUSNAVEUR LONDON UK//00/01/N3//  
COMSIXTHFLT  
COMHSTBATGRU  
CTF 60  
COMDESRON TWO  
NAVCRIMINVSERVFO EUR NAPLES IT  
HQ USEUCOM VAHINGEN GE//ETCC/ECJ2/ECSM//  
JAC MOLESWORTH RAF MOLESWORTH UK//DOA//

C O N F I D E N T I A L //N03800//

MSGID/GENADMIN/NEVERSAIL/-/FEB//

SUBJ/LOGREQ SECURITY SUPPLEMENT FOR (LOCATION) DATES(U)//

REF/A/DOC/USCINCEUR OPORD 01-01/DTG//

REF/B/GENADMIN/OPTASK FORCE PROTECTION-ANTITERRORISM  
(FP-AT)/DTG//

REF/C/DOC/NCIS ASSESSMENT/DTG//

NARR/(U) REF A REQUIRES SUBMISSION OF SUBJ SUPPLEMENT LOGREQ. REF B

**E-2-B-1**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

IMPLEMENTS FORCE PROTECTION CONDITION BRAVO FOR C6F AOR. REF C IS MOST RECENT NCIS THREAT ASSESSMENT FOR (LOCATION).

POC: //

RMKS/1. (U) IAW REFS A AND B, THE FOLLOWING SPECIAL SECURITY SUPPLEMENT F IS SUBMITTED FOR USS NEVERSAIL PORT VISIT TO (LOCATION), (DATES).

2. (U) IN VIEW OF FORCE PROTECTION GUIDANCE, THREAT ASSESSMENTS, AND ESTABLISHED FORCE PROTECTION CONDITION DETAILED IN REFERENCES, THE FOLLOWING SECURITY MEASURES REQUIRE COORDINATION WITH USDAO/COUNTRY TEAM AND HOST NATION:

- A. (U) REQUEST HOST NATION PROVIDE CONCRETE BARRIERS AND STEEL FENCING TO ESTABLISH AN EXCLUSION ZONE ON THE PIER, AND KEEP VEHICLES AT LEAST 400 FT FROM THE SHIP.
- B. (U) REQUEST HOST NATION AUTHORITIES CONDUCT INSPECTIONS OF ALL VEHICLES PRIOR TO ENTERING PIER.
- C. (U) REQUEST HOST NATION AUTHORITIES PROVIDE ARMED SECURITY AT THE ENTRANCE TO THE PIER.
- D. (U) REQUEST HOST NATION AUTHORITIES POST SIGNS IN LOCAL LANGUAGE PROHIBITING GENERAL VISITING AND LOITERING WITHIN 400 FEET OF THE SHIP.
- E. (U) REQUEST HOST NATION AUTHORITIES PROVIDE PICKET BOAT (SMALL MANEUVERABLE VESSEL) 24 HOURS A DAY, DURING NEVERSAILS VISIT, TO PREVENT UNAUTHORIZED VESSELS FROM CLOSING WITHIN 25 METERS OR MUTUALLY AGREED UPON DISTANCE. IF REQUEST CANNOT BE ACCOMMODATED, REQUEST TO PLACE NEVERSAIL'S UNARMED BOAT IN WATER TO PROVIDE WATERBORNE SECURITY PERIMETER.
- F. (U) REQUEST HOST NATION AUTHORITIES PROVIDE OIL BOOM OR BUOY LINE TO CLEARLY MARK WATERBORNE EXCLUSION ZONE.
- G. (U) REQUEST HOST NATION AUTHORITIES OR USDAO PROVIDE PRE-RECORDED WARNING TAPES REQUESTING WATERCRAFT TO REMAIN CLEAR OF THE SHIP.
- H. (U) REQUEST HOST NATION AUTHORITIES INSPECT AND CERTIFY PILOT BOATS, TUGS, WATERBORNE TAXIS AND BARGES IMMEDIATELY PRIOR TO LEAVING THEIR SLIPS ENROUTE TO NEVERSAIL. VERIFY NO AFFILIATION WITH EXTREMIST GROUPS, AND THAT CRAFT ARE FREE OF IEDS, OTHER EXPLOSIVES AND WEAPONS. IF REQUEST CANNOT BE ACCOMMODATED, REQUEST TO UTILIZE SHIP'S COMPANY TO INSPECT ALL WATERCRAFT PRIOR TO APPROACHING WITHIN 200 METERS OF THE SHIP.
- I. (U) REQUEST HOST NATION AUTHORITIES INSPECT AND CERTIFY PIER IS FREE FROM IEDS AND EXPLOSIVES, PRIOR TO NEVERSAIL'S ARRIVAL.

3. (U) REQUEST USDAO ADVISE NEVERSAIL VIA NAVAL MESSAGE, INMARSAT CALL TO CALLSIGN "XXXXXX" AT (PHONE NUMBER), OR EMAIL TO XXXXXX, AND ADVISE IF ANY OF THE ABOVE MEASURES CAN NOT BE MET BY HOST NATION.//

4. (U) INFORMATION HANDLING INSTRUCTIONS: ALTHOUGH THE CLASSIFICATION OF THIS MESSAGE IN ITS ENTIRETY IS CONFIDENTIAL BASED UPON COMPILATION RULES, INFORMATION IN INDIVIDUAL PARAGRAPHS IS FOR OFFICIAL USE ONLY (FOUO), AND AS SUCH, MAY BE RELEASED TO THE HOST NATION AND OTHER UNCLEARED PERSONNEL STRICTLY ON A NEED TO KNOW BASIS.

DECL/X1//

BT

NNNN

**E-2-B-2**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### TAB C (EXAMPLE OF INPORT SECURITY PLAN APPROVAL) TO APPENDIX 2 (SECURITY FOR IN-TRANSIT SHIPS) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPORD 01-01

**GENERAL.** The following example is provided to illustrate the format and typical content of an Inport Security Plan (ISP) approval message. This example is not all inclusive, and is provided only as an example. Although it is written as a classified message since the actual ISP approval message would normally be classified at CONFIDENTIAL, none of the information in this example is classified.

#### Example of Inport Security Plan (ISP) Approval Message

FM COMSIXTHFLT

TO CTF 60  
INFO CINCUSNAVEUR LONDON UK//N3/N34//  
USS DEYO  
NAVCRIMINVSERVFO EUR NAPLES IT//EUNA/FCI//  
COMSIXTHFLT  
HQ USEUCOM VAIHINGEN GE//ETCC/ECJ2/ECSM//  
JAC MOLESWORTH RAF MOLESWORTH UK//DOA//

C O N F I D E N T I A L //N00000//

MSGID/GENADMIN/COMSIXTHFLT/(MONTH)//

SUBJ/ ISP APPROVAL FOR (LOCATION) (U)//

REF/A/DOC/USCINCEUR OPORD 01-01/DTG//

REF/B/MSG/USS NEVERSAIL/INPORT SECURITY PLAN FOR (LOCATION)/DTG//

NARR/(U) REF A IS ANTITERRORISM/FORCE PROTECTION (AT/FP) GUIDANCE FOR USEUCOM AOR. REF B IS USS NEVERSAIL PROPOSED INPORT SECURITY PLAN FOR VISIT TO (LOCATION).//

POC/NESSER/CDR/C6F/AFPO/626-9000 X 6919,6917/  
SIPR:C6FN335(AT)C6F.NAVY.SMIL.MIL//

RMKS/1. (C) PER REF A, REF B IS APPROVED. ITEM 55 (ENERGIZING SONAR) WILL REQUIRE HOST NATION (HN) CERTIFICATION THAT SWIMMERS AND DIVERS ARE NOT IN THE VICINITY.

2. (C) PER REF A, AND AS ALWAYS, EVERY EFFORT SHOULD BE MADE TO ESTABLISH SECURITY ARRANGEMENTS WITH HN AUTHORITIES THAT PERMITS HN FORCES TO BE THE FIRST TO CONFRONT AN ATTACK. REF C PROVIDES SPECIFIC GUIDANCE TO BE FOLLOWED WHEN ESTABLISHING WATERBORNE SECURITY.

3. (U) INFORM C6F OF RESOLUTION OF AT/FP MEASURES AFTER COORDINATION WITH HN AUTHORITIES. REPORT INSTANCES WHERE YOU ARE UNABLE TO COMPLY WITH PUBLISHED GUIDANCE. INCLUDE REASON YOU CANNOT COMPLY, AND ALTERNATIVE AT/FP MEASURES IMPLEMENTED TO MITIGATE THE RISK.//

DECL/X1//

BT

NNNN

**E-2-C-1**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**E-2-C-2**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**TAB D (SECURITY ASSESSMENT SURVEY FORM AND CHECKLIST FOR  
NON-U. S. MILITARY PORTS) TO APPENDIX 2 (SECURITY FOR IN-TRANSIT  
SHIPS) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP  
OPORD 01-01**

The following survey form and checklist are provided to assist in conducting security assessments of port facilities. When completed, the information should be marked, as a minimum, "FOR OFFICIAL USE ONLY".

# FOR OFFICIAL USE ONLY

## SECURITY ASSESSMENT SURVEY FORM AND CHECKLIST FOR NON-U. S. MILITARY PORTS

Name of Port Assessed:

---

**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 should not be addressed as "fact".

Date(s) of Assessment:	
Assessment Member(s) (include contact information)	
Name	Contact Information
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

### SECTIONS

- I PERSONS INTERVIEWED/CONTACT INFORMATION POC LIST
- II THREAT INFORMATION
- III DETAILED PORT INFORMATION
- IV ENGINEERING
- V SECURITY FORCES
- VI DIVING OPERATIONS/ANTI-SWIMMER
- VII PORT SERVICES
- VIII SECURITY PLANNING AND PROCEDURES
- IX AIR FACILITIES (See Airfield Assessment Checklist in Annex E, Appendix 1, Tab F.)



# FOR OFFICIAL USE ONLY

## 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 FOR 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. Force Protection Condition 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:
2. Will foreign crewmen transiting nearby areas of concern to U.S. warships?
3. Will cargo be off-loaded/on-loaded and/or stores be co-located with US cargo/supplies?



**FOR OFFICIAL USE ONLY**

**SECTION III  
DETAILED PORT INFORMATION**

Port/Base/Pier/Anchorage/Fleet Landing/Seaman Centers: \_\_\_\_\_

**GENERAL GUIDANCE:** *This tab should be filled out with the intent to include all possible areas and buildings that U.S. Military Personnel will have interaction with while conducting Physical Security and Ships Business. Each item identified will be assessed for on the Physical Security/Force Protection/Engineering TABS. (Note: Tab VII will describe in more detail places of interest while on liberty.) Redundancy has been engineered into the tabs for maximum coverage of all areas of concern. Each tab should filled out by multiple team members.*

Dates: \_\_\_\_\_

ASSESSMENT MEMBERS:

NAME	CONTACT INFORMATION/TELEPHONE NUMBER(S)

PERSONS INTERVIEWED FOR THIS SECTION:

NAME	TITLE/POSITION	CONTACT INFORMATION/ ADDRESS/TELEPHONE NUMBER (S), ETC.

**NOTE:** *This portion of the tab should reflect all items of interest in providing Physical Security. Indicate HN 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 should not be addressed as "fact".*

**DETAILED PORT DESCRIPTION**

1. Port:
  - a. Location:
  - b. Name/address/designation:

## FOR OFFICIAL USE ONLY

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/Floorplans
  - 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

## FOR OFFICIAL USE ONLY

(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?

e.

E-2-D-7

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

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

U.S. Airfield

Commercial Hospital

Host Nation Military Hospital

U.S. Hospital

# FOR OFFICIAL USE ONLY

## SECTION IV FACILITY ENGINEERING

Port/Base/Pier/Anchorage/Fleet Landing/Seaman Centers: \_\_\_\_\_

(NOTE: Multiple filled Engineering Tabs should be incorporated into one File and Document for submission to the PVAT Program Manager.)

Date(s): \_\_\_\_\_

ASSESSMENT MEMBERS:

NAME	CONTACT INFORMATION/TELEPHONE NUMBER(S)

PERSONS INTERVIEWED FOR THIS SECTION:

NAME	TITLE/POSITION	CONTACT INFORMATION/ ADDRESS/TELEPHONE NUMBER(S), ETC.

**Note:** This TAB should be referenced for each item listed in TAB III, especially Medical Facilities. 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 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:

## FOR OFFICIAL USE ONLY

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?

## **FOR OFFICIAL USE ONLY**

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.

## **FOR OFFICIAL USE ONLY**

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?



## FOR OFFICIAL USE ONLY

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 size are there and are adapters required?

# FOR OFFICIAL USE ONLY

## SECTION V SECURITY FORCES

Port/Base/Pier/Anchorage/Fleet Landing/Seaman Centers: \_\_\_\_\_

(NOTE: Multiple filled Security Forces tabs should be incorporated into one File and Document for submission to the PVAT Program Manager.)

### ASSESSMENT MEMBERS:

NAME	CONTACT INFORMATION/TELEPHONE NUMBER(S)

### PERSONS CONTACTED FOR THIS SECTION:

NAME	TITLE	CONTACT INFORMATION/ ADDRESS/TELEPHONE NUMBER(S), ETC.

**Note: This TAB should be REFERENCED for each Item listed in TAB III, Especially Medical Facilities! Also pay attention 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 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):

## FOR OFFICIAL USE ONLY

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?
  - e. 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?
- d. Are EOD divers available?  
If "Yes", how may their services be arranged?
3. Is the U.S./HN security force training up to date?  
(Personal observation, if possible, may be necessary)
4. Is the U.S./HN security force armed?  
If "Yes", describe the weapon(s) carried and is there use of deadly force training:
5. Do U.S./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 U.S./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 and 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.?

## FOR OFFICIAL USE ONLY

- 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 pierside?
  - 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?

## **FOR OFFICIAL USE ONLY**

### **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?
3. 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:
4. 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?
3. Will a HN police representative accompany or be posted with the Shore Patrol and/or Beach Guard?

# FOR OFFICIAL USE ONLY

## SECTION VI DIVING OPERATIONS/ANTI-SWIMMER

Port/Base/Pier/Anchorage/Fleet Landing/Seaman Centers: \_\_\_\_\_

Dates: \_\_\_\_\_

ASSESSMENT MEMBERS:

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 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?

## FOR OFFICIAL USE ONLY

- 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 MediVac 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 prior to the ship's arrival?
  - d. Can (or will) EOD conduct period sweeps of the pier and/or hull while at berth or anchorage?

**FOR OFFICIAL USE ONLY**

**SECTION VII  
PORT SERVICES/HUSBANDING AGENTS**

Facility: \_\_\_\_\_

**General Guidance:** *One copy of this tab should be filled out by the Husbanding Agent and submitted to the PVAT. The PVAT is responsible for their own submission. This will give a wider scope of data input.*

**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 should not be addressed as "fact".*

Dates: \_\_\_\_\_

**ASSESSMENT TEAM MEMBERS:**

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 from inspecting tugs, support vessels prior to approaching the ship?
3. Are camels or other breasting out devices in good condition and can they be inspected by US and/or HN authorities?



## FOR OFFICIAL USE ONLY

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; Greek Navy, Husbanding Agent, etc.)? If Yes, Describe each and who controls coordinating it's 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?
7. Can the hours of operation for these vessels be regulated?
8. Are security measures in place to protect hotel services (e.g., electrical power, communications, water, etc.)?
9. Are visitors required escorts onto restricted areas?
10. Are protective barriers available for Ships? If Yes, Describe. (Sizes, dimensions, type)
12. Are reports and complaints handled quickly by HN/Port Ops?
13. Does limited number of roads restrict accesses to the port? Describe.
14. Is access to the port is limited to water borne vessels?
15. Are there 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, cities, 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?

**FOR OFFICIAL USE ONLY**

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?

# FOR OFFICIAL USE ONLY

## SECTION VIII SECURITY PLANNING AND PROCEDURES

Port: \_\_\_\_\_

Dates: \_\_\_\_\_

### ASSESSORS FOR 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, force protection, 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?

## **FOR OFFICIAL USE ONLY**

5. 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?

## FOR OFFICIAL USE ONLY

### APPENDIX 3 (SECURITY FOR IN-TRANSIT GROUND FORCES) TO ANNEX E (SECURITY OF IN-TRANSIT FORCES) TO USCINCEUR AT/FP OPORD 01-01

- 1. PURPOSE.** To ensure the effective planning and execution of Antiterrorism/Force Protection (AT/FP) measures for DoD ground forces transiting in or through the EUCOM AOR.
- 2. APPLICABILITY.** This Appendix applies to all ground units that could present lucrative terrorist targets, minimally those units or groups consisting of more than 50 personnel, or larger DoD elements conducting ground operations or ground movements in the USEUCOM AOR, and for which USCINCEUR has force protection responsibility. Commanders are encouraged to apply these measures to lesser movements when time and resources permit.
- 3. POLICY.** Although USCINCEUR exercises TACON for force protection over all DoD elements and personnel assigned, attached, or transiting through the USEUCOM AOR and not under the security authority of a Chief of Mission (COM), commanders at all levels are inherently responsible for the security of their forces. This Appendix provides directive guidance to commanders and outlines the minimum force protection requirements for transiting units.

#### 4. ASSESSMENTS

**a. General.** Prior to 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. This requirement applies to operations to or through areas where the Terrorism Threat Level is Significant or High, or where a geographically specific Terrorism Warning Report is in effect, and for all operations involving an airfield or port. Pending full implementation of the USEUCOM Joint Risk Assessment Management Program (JRAMP) and Ground RAMP database, commanders must view the USAREUR Force Protection Web Site on the SIPRNet at [www.odcsops.hqusareur.army.smil.mil/Divisions/OpsDiv/ForceProtection/docstobeshared.htm](http://www.odcsops.hqusareur.army.smil.mil/Divisions/OpsDiv/ForceProtection/docstobeshared.htm) for previous assessments on specific ground locations and routes. Airfield assessments and related information can be found on the HQ USAFE airfield RAMP database at <http://coldfusion.ramstein.af.smil.mil/RAMP/index.cfm>. Coordinate directly with HQ USNAVEUR and COMSIXTHFLT to obtain information on previously assessed ports until the USNAVEUR port RAMP database is operational. Current assessment data and force protection related information for ports can be found at [www.naveur.navy.smil.mil/n3/n34.html](http://www.naveur.navy.smil.mil/n3/n34.html) and [www.205.39.230.71/fp/](http://www.205.39.230.71/fp/). Additional sources of assessment information include the Country Team at the U.S. Embassy, and various component command headquarters.

**b. On-site assessment.** After conducting a preliminary assessment, which normally includes checking available ground, airfield and port databases, commanders must determine if an on-site force protection assessment is

## FOR OFFICIAL USE ONLY

required. Assessment team composition is mission and location dependent, with specific functional area representation potentially including operations, intelligence/counterintelligence, physical security, terrorist operations, 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.

**c. Assessment Checklist.** Attached at Tab A is a sample Assessment Checklist/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 force protection-specific considerations related to ground transit operations.

**d. Assessment Locations.** Ground transit operations in the USEUCOM AOR will typically begin at an aerial port of debarkation (APOD) or seaport of debarkation (SPOD). Coordinate with HQ USAFE and/or HQ USNAVEUR to acquire any assessment data they may have, and update their information as necessary. However, the component command ground assessment will include data that is not routinely collected in conjunction with a USAFE or USNAVEUR assessment. The focus on protecting personnel conducting ground operations, versus flight or naval operations, requires additional assessment criteria oriented to the threat specific to the ground portion of the mission.

(1) Rail movements typically support transfer of equipment in the USEUCOM AOR. However, on-load/off-load operations are considered transit operations, and component commands must conduct assessments and develop security plans for railhead operations.

(2) 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.

(3) Forward-deployed units conducting missions or exercises rarely remain confined on a base camp. The installation or base camp AT/FP plan should address security measures for operations at the base camp, while the requirements in this Appendix apply to movements of forces away from the operating location, that are not integral to the mission or to the execution of the base camp security plan. For short-duration missions or exercises, the base camp itself is considered a transit location requiring assessment and development of a security plan under the provisions of this Appendix.

**5. MOVEMENT SECURITY PLANNING.** Commanders will develop a movement security plan focused on in-transit operations and synchronize this

## FOR OFFICIAL USE ONLY

plan with the overall movement plan. The security plan must include specific measures addressing:

**a.** 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 equipments, and vehicle escort and movement requirements. For repetitive movements, consider varying routes and times to prevent establishing a routine that facilitates terrorist planning.

**b.** Procedures for maintenance recovery operations, including security of the recovery team.

**c.** Procedures for medical evacuation, including security of the medical team.

**d.** Command and control/communications. 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.

**e.** Rules of engagement for each country or area that the element will transit or occupy.

**f.** Provisions for Host Nation security support, when appropriate. Host nation police or military can be an invaluable asset to transiting units, as local forces generally have a much greater understanding of the threats to transiting forces.

**g.** Operations Security. 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.

**6. THREAT WORKING GROUP/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.

**a.** To ensure the decision to conduct operations is made at the appropriate level, component commanders will establish policies and procedures to ensure the component command and appropriate subordinate command headquarters have a formal process to assess risk, including specific approval authority for

## FOR OFFICIAL USE ONLY

each level of risk. All high-risk movements require General/Flag Officer approval prior to execution. Movements considered to be "high-risk" may include those involving particularly sensitive resources or high-risk personnel, or movements in areas where the Terrorism Warning Reports have been issued or the Threat Level is Significant or High

b. Frequently occurring high-risk movements do not require General/Flag Officer approval for each movement. The initial movement briefing will include information on planned future movements, and the General/Flag Officer may approve future operations contingent upon continuously updated risk assessments that determine no change in risk level.

**7. PRE-DEPLOYMENT TRAINING.** Transiting elements must complete all required training prior to arrival in theater or movement. Although parent units are responsible for training their forces, the commander responsible for force protection during the operation must ensure all forces have completed the required training. Mandatory training includes:

a. Completion of Level I AT/FP training for all personnel.

b. Completion of Level II AT/FP training for each battalion/separate company, squadron, or ship Antiterrorism Officer (ATO).

c. Individual and collective training on all tasks supporting the security measures contained in the security plan. Training should be performance-oriented, and include vignettes and antiterrorism scenarios to provide challenging and realistic training.

d. Review of the Rules of Engagement for all countries or areas the element will transit or occupy. Training must include scenarios that require forces to apply the rules of engagement in various scenarios they are likely to encounter while transiting.

e. Comprehensive country or area threat briefs.

f. Training on all weapons and equipment that the element may use in the execution of security measures.

**8. IN-TRANSIT OPERATIONS.** 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.

**9. POST-DEPLOYMENT AFTER ACTION REPORTS (AAR).** For all operations outside of Germany, Italy or the BENELUX, units must provide After Action



## **FOR OFFICIAL USE ONLY**

Reports electronically to the HQ USAREUR Force Protection Branch within 60 days after completion of movement. These After Action Report must include the written threat and vulnerability assessments, and the movement security plan. HQ USAREUR will maintain these products on the Force Protection web site (<http://www.odcsops.hqusareur.army.smil.mil/Divisions/OpsDiv/ForceProtection/index.htm>) until the USEUCOM JRAMP becomes completely operational.

### **ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
**General, USAF**

### **TAB:**

A. Assessment Checklist for In-transit Ground Forces

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**E-3-6**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**TAB A (ASSESSMENT CHECKLIST FOR IN-TRANSIT GROUND FORCES)  
TO APPENDIX 3 (SECURITY FOR IN-TRANSIT GROUND FORCES) TO  
ANNEX E (SECURITY OF IN-TRANSIT FORCES) USCINCEUR AT/FP OPOD  
01-01**

<b>Assessment and Security Planning Considerations</b>		
What is the DIA/USEUCOM 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 soldiers 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.		

**FOR OFFICIAL USE ONLY**

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 Host Nation 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 (Host Nation, U.S. contractor, military, police)?		
Who is responsible for C2 of force protection, if the task force occupies facilities with Host Nation or friendly forces?		
How reliable and well-trained are Host Nation forces?		

**FOR OFFICIAL USE ONLY**

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 Force Protection Condition measures in the AOR need to be modified or supplemented? What are the unit responsibilities under each Force Protection Condition?		
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)?		
<b>Security Plan</b>		
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 Force Protection Condition and establish locally tailored, mission specific measures and standards.		

## FOR OFFICIAL USE ONLY

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 vulnerability assessments 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 Force Protection Condition 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.		
Determine which checkpoints and barriers are necessary to control compound access and ensure adequate standoff.		

**FOR OFFICIAL USE ONLY**

Determine where will mission essential vulnerable areas (MEVA) be established. Identify their vulnerability to attacks or observations.		
<b>Pre-Deployment Training and Exercises Must Include:</b>		
Completion of Level I AT/FP training or refresher training within the past year for all personnel.		
Completion of Level II AT/FP 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.		

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**E-3-A-6**  
**FOR OFFICIAL USE ONLY**



**FOR OFFICIAL USE ONLY****ANNEX F (PUBLIC AFFAIRS) TO USCINCEUR AT/FP OPORD 01-01****REFERENCES: See Basic Order**

- 1. General.** This Annex provides guidance governing Public Affairs (PA) concerning Antiterrorism/Force Protection (AT/FP) and Counterterrorism (CT) operations.
- 2. Policy.** The USG considers all terrorist acts to be criminal acts. The USG will make no concessions to terrorists. The USG will not pay ransom and will identify and isolate those nations fostering terrorism. Because of this governmental posture, the measures delineated in this Annex to combat terrorism may arouse intense international interest.
- 3. Lead Agency.** DOS is the lead agency for responding to international terrorist incidents that involve U.S. citizens, DoD elements and personnel, and facilities outside of the United States. The Federal Aviation Administration (FAA) is responsible for terrorist incidents that affect the safety of DoD personnel or property aboard aircraft in flight. It may not be possible to preclude the dissemination of information concerning a particular terrorist group and its activities. However, it is imperative to protect information concerning U.S. elements, personnel, equipment, weapons, and tactics associated with combating terrorism.
- 4. Reporting.** In addition to operational reporting requirements, report all terrorist incidents through the chain of command immediately to HQ USEUCOM ECPA for referral to the office of the Assistant Secretary of Defense, Public Affairs (OASD (PA)) who is the single point of contact for releasing information to the public. Do not make any public release of information concerning a terrorist incident without OASD (PA) approval except for cases involving public safety.
- 5. Training and Awareness.** To support DoD-directed AT/FP briefings and training requirements, commanders at all levels should work closely with their Public Affairs staffs to use all available internal information resources, in addition to chain-of-command communication, to distribute AT/FP information. Such resources include, but are not limited to commercial enterprise newspapers, commanders' call topics, installation/command Internet home pages, and submissions to Armed Forces Network (AFN).
  - a.** Prior to taping AFN TV or radio AT/FP commercials, AFN Europe and component commands are strongly encouraged to forward proposed scripts to the HQ USEUCOM Special Assistant for Security Matters (ECSM) for review and correlation. This does not apply to AT/FP messages disseminated through command information channels and in no way should infringe upon a commander's prerogative to communicate rapidly and directly with subordinates. Rather, this review process is designed to ensure AT/FP messages are consistent, effective, and comply with DoD and USCINCEUR AT/FP policies, as well as being responsive to the most recent emerging threats. Additionally, ECSM, in coordination with ECPA, will issue AT/FP PA guidance that includes talking points and key themes and messages.

**FOR OFFICIAL USE ONLY**

b. Commanders should also be aware external media, such as the *European Stars and Stripes* and Host Nation broadcast and print media, may take an interest in AT/FP exercises and events. Commanders should use these opportunities to increase AT/FP awareness by delivering command AT/FP messages to the public through the external media in coordination with their PA staffs.

**6. Antiterrorism.** The following guidance is applicable when responding to media requests for information pertaining to antiterrorist activities:

a. If contacted directly by a media representative, refer him/her to the Public Affairs Office.

b. Subordinate commanders may discuss the subject of antiterrorism as it pertains to those areas/installations/sites for which they have responsibility. However, discuss antiterrorist measures and procedures only in general terms without going into specific details.

c. Incidents of terrorism and crime will generate external media interest. In response to queries concerning a possible or real terrorist threat at a particular activity, installation, or community, the commander may acknowledge that increased security measures have been or will be taken without going into specific details regarding the measures being taken. It may be appropriate and operationally sound to acknowledge the obvious. For example, increased AT/FP measures such as additional guards at the gate and/or more stringent identification checks are usually obvious to the public, and acknowledgment may serve to send a positive message of increased readiness. Commanders should exercise care and prudent judgment in any discussion of these or other security measures to preclude revealing tactics and techniques that an adversary could exploit. Commanders will respond to media inquiries through their PA offices to ensure compliance with DoD and Service directives.

d. Unless special circumstances apply, unclassified elements of public affairs guidance may be routinely posted to the USEUCOM unclassified web site IAW established USEUCOM and DoD policies and regulations. Certain items of sensitive, but unclassified, information should not be made available to the public, including details of AT/FP measures.

**7. Counterterrorism**

a. Use the following statement in response to queries regarding counterterrorist forces within USEUCOM: "The U.S. government has equipment and trained forces from all four services and the functional CINCs designated to cope with terrorist incidents. Also, command and control elements for these forces exist and have been exercised. These elements report to the Joint Chiefs of Staff, as do other command and control elements for military operations. We do not comment on any details concerning the circumstances under which these forces may be deployed, their identity, or their tactics."

**FOR OFFICIAL USE ONLY**

**b.** If contacted directly by a media representative, refer him/her to the Public Affairs Office.

**8. Medical.** Public Affairs information on the medical aspects of AT/FP should be readily available.

**9. Other PA Procedures.** See the USEUCOM Standard Plan 4000.

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
General, USAF

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

# FOR OFFICIAL USE ONLY

## ANNEX J (COMMAND RELATIONSHIPS) TO USCINCEUR AT/FP OPORD 01-01

### REFERENCES: See Basic Order

**1. General.** This Annex provides a chart diagram on page J-2 which illustrates command and control relationships for USEUCOM during routine operations and exercises. The diagram also illustrates AT/FP coordination responsibility. For contingency and other wartime operations, USCINCEUR will specify command relationships in appropriate OPORDs and EXORDs.

**2. Command Lines.** Combatant Command (COCOM and OPCON) authority entails AT/FP responsibility. Service component commands, Task Force (TF) or Joint Task Force (JTF) commanders, senior U.S. officials in Combined Task Forces (CTF), or the Chief of Mission (COM) may have AT/FP responsibility for designated DoD elements and personnel. These responsibilities and relationships are detailed in CINC-COM Memoranda of Agreements (MOA) and accompanying matrix showing AT/FP lines of responsibility, which serve as the formal delegation of TACON for force protection from USCINCEUR to subordinate commanders.

**a.** Each Service component commander who is identified as having TACON for force protection in the matrix accompanying a given CINC-COM MOA may further delegate this authority to subordinate commanders.

**b.** See paragraph 5 of the Basic Order for additional information regarding command relationships, to include the concept of TACON for force protection.

### ACKNOWLEDGE

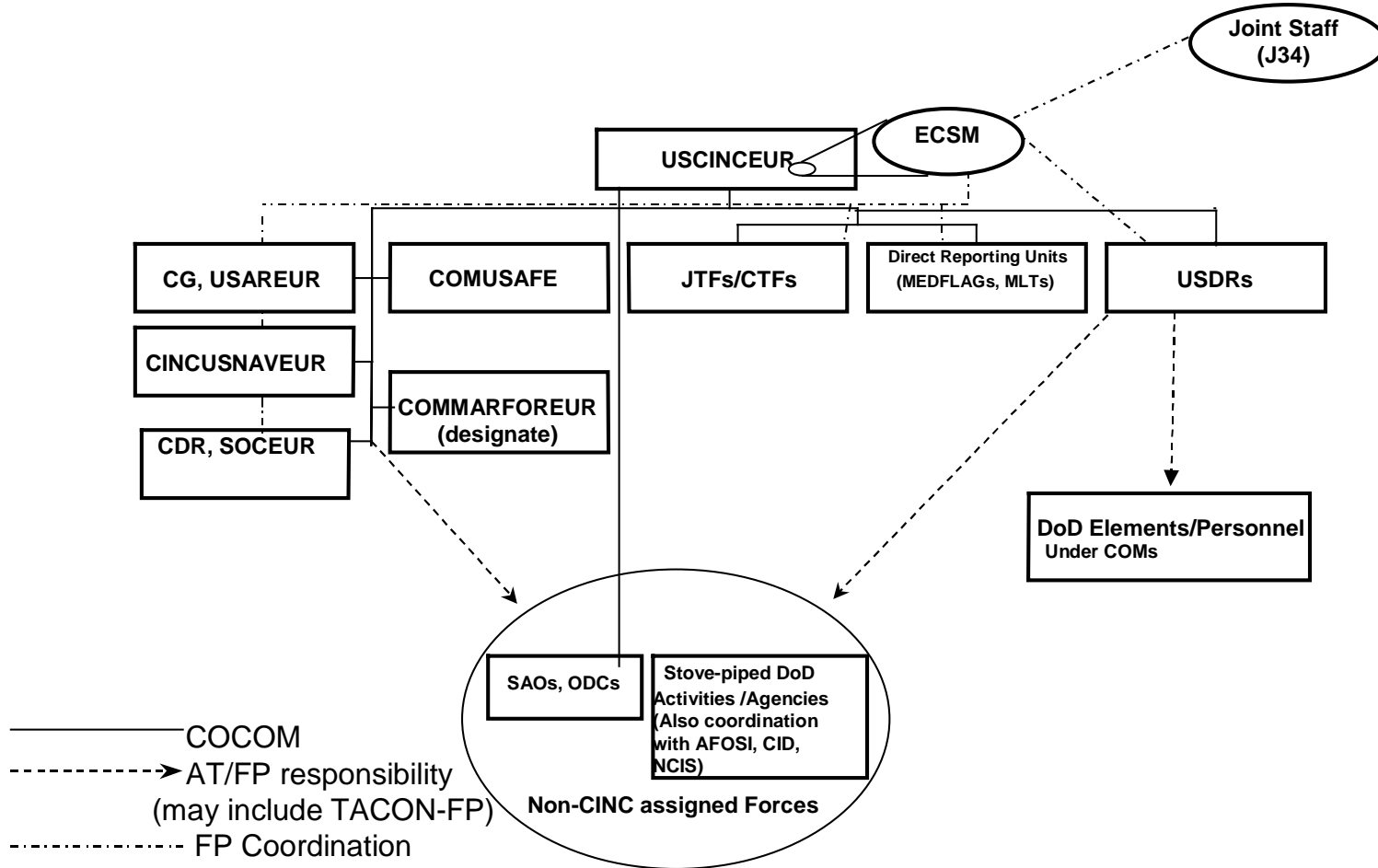
**JOSEPH W. RALSTON**  
General, USAF

# AT/FP Command Relationships and Coordination Channels

FOR OFFICIAL USE ONLY

J-2

FOR OFFICIAL USE ONLY



## FOR OFFICIAL USE ONLY

### ANNEX K (DEFENSIVE INFORMATION OPERATIONS) TO USCINCEUR AT/FP OPORD 01-01

<b>REFERENCES:</b>	<ul style="list-style-type: none"><li>a. DOD Directive S-3600.1 Information Operations, 9 Dec 96</li><li>b. USEUCOM Directive (ED) 25-5, Information Assurance</li><li>c. USEUCOM ED 100-1, Defensive-Information Warfare, 10 Feb 97</li><li>d. Joint Pub 3-13, Joint Doctrine for Command and Control Warfare (C2W), May 97</li><li>e. Joint Pub 3-54, Joint Doctrine for Operations Security, Jan 97.</li><li>f. FM-100-6, Information Operations, Aug 96</li><li>g. USEUCOM ED 55-11, Joint Task Force Headquarters Policies, Procedures, and Organization, 7 July 95</li></ul>
--------------------	--

**1. SITUATION.** This Annex provides guidance on the defense of automated information and information systems from terrorist attack. The Secure Internet Protocol Router Network (SIPRNet) and Non-secure Internet Protocol Router Networks (NIPRNet) provide this command with an unprecedented ability to share information and intelligence. Members of this command must be vigilant to ensure the SIPRNet is not compromised and the NIPRNet does not house or transmit classified data or violate OPSEC.

**2. MISSION.** To provide appropriate command and control (C2)-protection elements in support of U.S. interests in USEUCOM AOR. To gain C2 Superiority and Supremacy by denying, negating, or turning to friendly advantage, adversary efforts to destroy, disrupt, or deny information to the U.S. and allied C2 systems, including its supporting communications, information, and intelligence activities.

### 3. EXECUTION

#### a. Scheme of Support

(1) Maintain effective C2-Protection of U.S. Forces by turning to friendly advantage or negating adversary efforts to deny information to influence, degrade, or destroy friendly C2 systems.

(2) Conduct C2-Protection operations by offensive or defensive means. Implement Offensive C2-protection using the five elements of C2W reducing the adversary's ability to conduct C2-attack. Implement Defensive C2-Protect measures by reducing friendly C2 vulnerabilities and adversary C2-attack through employment of adequate physical, electronic, and intelligence protection.

(3) **Phasing.** Operational deployments of Joint Task Forces (JTF) shall normally be phased as follows:

K-1

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

**(a) Phase I - Pre-hostilities.** HQ USEUCOM ECJ6 shall serve as the focal point for C2-Protection pre-deployment planning.

**(b) Phase II - Lodgement.** Designated forces under the command and control of Force/JTF Commander shall deploy as required and prepare for the C2-protection mission execution. ECJ6 will ensure C2-protection is adequately planned and protected.

**(c) Phase III - Operations.** ECJ6 shall maintain and determine the availability of C2-protection connectivity assets and ensure that all components are aware of those assets. USEUCOM activities during this phase coordinate development of specific plans for the elements of C2-protection among the organizations responsible for the elements.

**(d) Phase IV - Follow-through.** ECJ6 shall recommend priorities for C2-protection to the HQ USEUCOM ECJ3/6 planners. Integration of all five elements of C2W makes C2-protection a powerful and important strategy.

**(e) Phase V - Post-hostilities and Redeployment.** Phase V end state: All C2-protection resources are safely redeployed.

### **b. Tasks and Responsibilities**

**(1) HQ USEUCOM ECJ2.** Advise HQ USEUCOM of the assessed threat.

#### **(2) HQ USEUCOM ECJ3**

**(a)** Establish Information Operations Conditions (INFOCON) as required, per Annex B, reference (b). As per reference (b), the decision to change INFOCON levels will be based on assessed threat, vulnerabilities, extant situation, and the effect the action would have on all operations within the USEUCOM AOR.

**(b)** Provide to ECJ6 Essential Elements of Friendly Information (EEFI) listings, frequencies, telephone numbers, terminal identification numbers and any other technical data required to perform Joint COMSEC Monitoring Activity as tasked to ECJ6.

#### **(3) HQ USEUCOM ECJ6**

**(a)** Advise ECJ3 on vulnerabilities to the SIPRNet and NIPRNet.

**(b)** Ensure networks are monitored for unauthorized entry.

**(c)** In coordination with ECPA, review USEUCOM NIPRNet websites for information that would compromise OPSEC.



## FOR OFFICIAL USE ONLY

(d) Coordinate with the Joint COMSEC Monitoring Activity to ensure COMSEC monitoring of enciphered and un-enciphered voice, facsimile, data, or other type of telecommunication systems in support of operation.

(4) **HQ USEUCOM ECPA.** Webmaster for the HQ USEUCOM NIPRNet homepages. Check postings to ensure classified or sensitive material that would violate OPSEC is not placed on the HQ USEUCOM NIPRNet homepage.

(5) **HQ USEUCOM ECSM.** Conduct spot checks of USEUCOM NIPRNet web sites.

(6) **HQ USEUCOM Information Operations Cell (IOC).** In coordination with the IO Cell Working Group, will recommend changes in INFOCON level to the USEUCOM ECJ3.

### (7) Service component commanders

(a) Develop and implement procedures to guard against sensitive information being posted on as well as links to other sites on both SIPRNet and NIPRNet web sites.

(b) Immediately report any efforts to enter secure domains by unauthorized users to HQ USEUCOM (ECJ6) and the appropriate proponent within the parent Service.

(c) Ensure compliance with Service/Component Command "Notification and Consent" procedures to allow telecommunications monitoring and assessment.

### d. Coordinating Instructions

(1) **Guiding Principles.** The following will be applied during mission planning and execution to ensure maximum effectiveness of C2-protection:

(a) **Integration.** To provide the maximum friendly C2-protection, C2-protection measures, and active counter-C2 actions. Integrate with C2W Battle Staff, joint commander/ECJ3 C2W Officer, ECJ2 Rep, ECJ6 Rep, EWO, ETCC/CAT, JFACC Rep and PSYOP Rep.

(b) **Coordination.** C2-protection planners shall integrate elements (deception, OPSEC, EW, PSYOP and Counter-C2) into friendly C2 communications resources.

(c) **Security.** Due to the sensitive nature of some aspects of C2-protection (such as military deception), all members of the IO cell shall have the appropriate security clearance and access necessary to fulfill their C2-protection responsibilities.

(2) **Secure Internet Protocol Router Network (SIPRNet).** The following rules will apply to ensure maximum security of the SIPRNet:

## FOR OFFICIAL USE ONLY

(a) Do not place compartmented or information classified higher than “SECRET” on the SIPRNet.

(b) All material deemed sensitive, but not compartmented, by the originator should be password protected. Examples of this are vulnerability assessment databases, such as the VAMP.

(c) SIPRNet is a U.S. Only system, foreign nationals may not be granted access.

(d) Do not disseminate NATO classified material via the SIPRNet. However, a NATO classified – RELEASABLE TO THE US document may be remarked classified –REL NATO before dissemination.

(3) Material that is unclassified may still assist terrorist or hostile elements in planning attacks against installations. Do not post specific information about installations, such as detailed installation maps or housing floor plans on unclassified web pages.

(4) Do not post or send material marked FOR OFFICIAL USE ONLY via the NIPRNet.

(5) Do not place or forward program files (executable files are typically those files with a “.exe” extension) on personal computers (whether unclassified or classified systems) that have not been distributed by the unit/activity system proponent for information systems (the proponent for HQ USEUCOM is ECJ6-CSC). These type programs include screensavers, animations, new tools, or “new” versions of existing tools. Prohibiting the use of unauthorized software will help prevent the spread of computer viruses as well as prevent the installation of a “backdoor” to gain unauthorized access to machines (programs otherwise known as “Trojan Horses”). If an administrator runs such a program, or if the program exploits a weakness, the backdoor can permit administrator or system-level access.

#### 4. ADMINISTRATION AND LOGISTICS

**a. Personnel.** Component Commands will request augmentation from Service IW/C2W organizations: Land Information Warfare Activity (LIWA), Air Forces Information Warfare Center (AFIWC), and Fleet Information Warfare Center (FIWC). Augmentation request for Joint Command and Control Warfare Center (JC2WC) support will go through HQ USEUCOM ECJ35 to ensure an effective service balance for conducting joint operations. SHAPE shall Validate NATO command and control warfare requests.

**b. Supply.** Sophistication of modern communications systems and equipment offers a significant advantage to commanders if used properly and protected adequately. C2-protect planners should not view communications as the only component of C2.

## **FOR OFFICIAL USE ONLY**

(1) C2 facilities and equipment, adequate connectivity, computer support, and interoperable databases are required for USEUCOM effective communications.

(2) Secure communications and data transfer should be incorporated at all locations wherever C2-protection planning occurs.

(3) Computer support, including automated decision aids, can assist C2-protection planners in planning and monitoring C2W operations.

### **ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
**General, USAF**

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**K-6**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### ANNEX L (USEUCOM AT/FP SECURITY CLASSIFICATION GUIDE) TO USCINCEUR AT/FP OPORD 01-01

- REFERENCES:**
- a. DoD Directive 5200.1, DoD Information Security Program, 13 Dec 96
  - b. DoD Regulation 5200.1-R, Information Security Program, 14 Jan 97
  - c. DoD Pamphlet 5200.1PH, Guide to Marking Classified Material, 28 Apr 97
  - d. DoD 5400.7R, Freedom of Information Act (FOIA), 29 Sep 97
  - e. NDP-1, National Policy and Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations (S/NF), 1 Oct 88

**1. PURPOSE.** This Annex provides guidance on classification and marking of information and materials generated in support of the implementation, management, and oversight of actions required by this OPORD.

**2. GENERAL.** This document contains sensitive information related to Antiterrorism and Force Protection (AT/FP) of DoD elements, to include personnel engaged in tactical operations in forward deployed environments. The document is marked to be handled FOR OFFICIAL USE ONLY, and the information contained herein must remain under the control of U.S. government. Electronic transmission of this document, and portions thereof, must be made over protected systems, e.g., the Secret Internet Protocol Router Network (SIPRNet) or higher. DoD directives strictly prohibit the transmission or revelation of information contained herein, in any manner, to an unauthorized person.

a. It is crucial that information generated and used in support of this OPORD not be over-classified, since it must be made readily available to those personnel and agencies responsible for implementation and/or correction. However, because of the far-reaching applicability of the requirements, care must be exercised to ensure that classified and sensitive unclassified National Defense information is not compromised. This is especially true in the USEUCOM AOR, where there are requirements to work closely with our allies and host nation, as well as other non-cleared personnel, to implement appropriate measures in support of the AT/FP program. To achieve a balance between making information available and yet providing sufficient protection, any AT/FP plan with a complete listing of site-specific AT/FP measures, linked to a Force Protection Condition, will be classified, as a minimum, CONFIDENTIAL. When separated from the AT/FP plan, specific AT/FP measures and Force Protection Conditions remain FOR OFFICIAL USE ONLY. Handling, storage and control of such

## FOR OFFICIAL USE ONLY

information must comply with the requirements contained in DoD 5200.1-R, Information Security Program Regulation, and DoD 5400.7R, Freedom of Information Act (FOIA).

**b.** Instructions contained in this guide are provided in three separate sections:

**(1)** Section I contains general information to assist the user in understanding terms and procedures for handling classified information.

**(2)** Section II contains classification guidance to be used when developing classification instructions for material generated when conducting AT/FP vulnerability assessments.

**c.** Reproduction of this document for local use, or distribution to higher headquarters and subordinate or other commands is authorized.

**3. AUTHORITY.** This Security Classification Guide (SCG) is issued under the authority of DoD Directive 5200.1, and DoD 5200.1-R, references (a) and (b). This SCG constitutes the authority for classification, regrading and declassification of information relating to the affected programs. Changes in classification required by application of this SCG shall be made immediately. Information classified in accordance with this SCG is by authority of the Commander in Chief, US European Command (USCINCEUR).

**4. APPLICABILITY.** This SCG applies to all information generated by assessments done within theater by component headquarters and other subordinate commands. Classification of Joint Staff Integrated Vulnerability Assessments (JSIVA) will be in accordance with the DTRA Force Protection Security Classification Guide, reference (e). Dated Information cited from another SCG or other derivative source that bears classification or other restrictive marking shall retain the original markings, classification and downgrading instructions. This is the process of *derivative classification*. All reports or information related to the USEUCOM AT/FP program normally should be marked and handled as FOR OFFICIAL USE ONLY, or other appropriate caveat for the type of information, unless classified at a higher level.

### 5. RELEASABILITY

**a.** Unclassified or unclassified sensitive information may be released to the host nation authorities on a "need to know" basis when it directly impacts on an organization's ability to implement the AT/FP program or correct noted deficiencies identified during a vulnerability assessment or program review.

**b.** Classified information that must be released to or shared with the host nation of the affected installation or location must be appropriately cleared through Foreign Disclosure channels to the National Military Information Disclosure Policy Committee. See NDP-1, National Policy and Procedures for Disclosure of Classified Military

L-2

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

Information to Foreign Governments and International Organizations, reference (d), for the proper procedures to follow when addressing this area. NDP-1 also contains listings by country of that information that has already been cleared for release.

### 6. DECLASSIFICATION

**a.** Classified information in reports generated by USEUCOM vulnerability assessment teams shall be declassified ten years from the date of publication of each assessment report, unless otherwise stated in this guide or other classification source. During the declassification process, information contained in those reports that is classified by other sources and/or is exempt from declassification, shall be removed from the reports and filed appropriately or destroyed. Exemption categories or declassification date/event must be typed or printed on the front page together with the classification authority and the reason for classification. See Section III, paragraph 4, below, for examples of proper marking of classified documents. Also, consult DoD Pamphlet 5200.1PH.

**b.** Documents or information generated by USEUCOM AT/FP assessment teams, and extracted from such reports, shall be automatically declassified at the same time as the report. Reports or other documents generated in support of the local or theater implementation of AT/FP programs will be downgraded/declassified in accordance with theater specific classification guidance and/or other classification sources used to classify information relating to weapons systems or other programs specific to the affected location or theater of operation.

# FOR OFFICIAL USE ONLY

## Section I General Discussion

### 1. Vulnerabilities

a. A major vulnerability is exposure of humans to loss of life or serious injury resulting from an act of terrorism. A major vulnerability may result from the exposure of a critical asset, such as water or food supplies to compromise or destruction. For example, if an isolated installation has but one water supply, that water supply is a critical asset. The probability of its contamination would constitute a major vulnerability.

b. A minor vulnerability is exposure of sensitive assets to compromise or destruction. For example, if the utilities in an underground command center were interrupted, eventually, fresh air would become unavailable.

### 3. Unclassified Information

a. The fact that certain information is marked UNCLASSIFIED may cause it to be authorized for public release. Therefore, information that should not be released to the general public, although unclassified, should be marked with the appropriate caveat for category of information contained. An example would be FOR OFFICIAL USE ONLY.

b. Information is marked UNCLASSIFIED when:

(1) It is not classifiable on its own merits at a given moment, but is included with or extracted from a classified document, or

(2) It has been reviewed by a classification management analyst because of a question about its classifiability, and found to be not classifiable at the time of review. It may, however, be classifiable when aggregated or compiled with other information.

c. Any information pertaining to official government functions or business is the property of the United States Government, and remains such until released into the public domain by proper authority.

### 4. Marking a Classified Document

All classified information, whether contained in a report, document, or briefing, or derived from a report shall be conspicuously marked with the appropriate level of classification. If information is unclassified, it must be conspicuously marked UNCLASSIFIED. Each classified document shall bear a classification authority, and a declassification date that is ten years from the date of the report, unless classified for a longer period by other pertinent classification source. The term OADR is no longer permitted. The following is the sample format to be used for information that is classified IAW this SCG, *and that contains no information classified by another source.*

L-4

FOR OFFICIAL USE ONLY



## FOR OFFICIAL USE ONLY

CLASSIFIED BY: USCINCEUR AT/FP OPORD 01-01, XX JAN 01  
REASONS: 1.5a and 1.5g.  
DECLASSIFY ON: 30 August 2010 [A date that is ten years from the date of the Report.]

A report that contains information classified by this SCG, in addition to information that is classified by other (or multiple) sources is called a document derivatively classified by multiple sources. To properly mark such a document, you *must* consult DoD 5200.IR, Chapter 5, Section 2, or DOD 5200.1-PH, Section 2.

### ADDITIONAL MARKING REQUIREMENTS

The following statement **MUST** be placed at the bottom of each report that is classified higher than any of its individual constituent portions:

*While the majority of portions in this document are unclassified on individual merit, this compilation of those portions is classified (SECRET) (CONFIDENTIAL) because it reveals vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security.*

# FOR OFFICIAL USE ONLY

## Section II Classification Topics

**Authority for Classification for each Topic:** Section 1.5 a. and Section 1.5 g.

**Declassification:** 10 years from date of report unless otherwise noted in Remarks or Notes.

TOPIC	CLASS OR EXEMPTION	REMARKS
<b>1. Scheduling &amp; coordination</b>		
<b>a. OCONUS</b>		
<b>(1)</b> If host country is on the Department of State Warning List (DSWL)	FOUO or C	Declassify on completion of trip. See Remarks Below
<b>(2)</b> If host country is not on the DSWL	U	
<b>Remarks:</b> Handle on a case-by-case basis to determine need for classification at the confidential level. This would normally be a consideration when a General/Flag Officer or civilian equivalent in a critical position accompanies the team. Also, it would be a consideration when traveling to certain "Significant or High" Terrorism Threat Level areas.		
<b>2. Administrative Preparation</b>		
<b>a.</b> Medical, Legal	U	
<b>b.</b> Orders	U	See Remarks Below
<b>Remarks:</b> If location to be visited is classified, specific information that is classified could be "data masked" so that travel orders may remain unclassified.		
<b>3. Assessment</b>		
<b>a.</b> In-brief	U, C or S	TBD by Team Leader See Remarks Below
<b>b.</b> Outbrief	U, C or S	TBD by Team Leader See Remarks Below
<b>Remarks:</b> If other classified topics are to be discussed, classification will be at the level determined by the briefing topics. Also, cumulative classification should be considered as described in NOTE 1 of the guide.		
<b>4. Post Assessment</b>		See Remarks Below
<b>a.</b> Final Report	U, C or S	See NOTE 1
<b>b.</b> Association of an identified major vulnerability with a named U.S. military site	C	
<b>c.</b> The mere existence of a major vulnerability, U.S. military site not identified by name or country of location	U	
<b>d.</b> Association of an identified minor vulnerability with a named U.S. military site	FOUO	
<b>e.</b> The mere existence of a minor vulnerability, U.S. military site not identified by name or country of location	U	

## FOR OFFICIAL USE ONLY

TOPIC	CLASS OR EXEMPTION	REMARKS
<b>5. Lessons Learned</b>		
a. Associated with a named U.S. military site	FOUO	
b. Not associated with a named U.S. military site (i.e., not in an outbrief, or in a written report)	U	
<b>6. Host Installation Physical Security</b>		See Remarks Below
<b>Remarks:</b> Normally classification would depend on the type resource being protected. In those instances, use other applicable classification guidance. In each of the issues addressed below, the team chief decides on classification level based on that guidance.		
a. The mere fact of existence of an intrusion detection system (IDS)	U	
b. The mere fact of non-existence of an IDS	U	OPSEC Sensitive
c. Details of type, dispersal, and power supply of IDS	U, C or S	TBD by Team Leader
d. Details of planned response to an intrusion alarm, whether test, false, or real	FOUO - CONFIDENTIAL	See Remarks Below
<b>Remarks:</b> Normally FOUO, but defer to guidance pertaining to specific resource being protected.		
e. Any information that reveals, or may tend to reveal vulnerabilities of an IDS	FOUO - CONFIDENTIAL	See Remarks Below
<b>Remarks:</b> Normally FOUO, but defer to guidance pertaining to specific resource being protected.		
f. Details revealing assigned ammunition load, ready loads, number of persons absent, morale, state of readiness.	U, C or S	See Remarks Below
<b>Remarks:</b> Classification of the aggregate of this type of information may be classified per NOTE 1, depending on the weapons system or program. Usually other classification guidance exists which normally would be used. The team chief would make these determinations based on that guidance.		
<b>7. Logistics: Billeting</b>	U - FOUO	Use OPSEC guidelines
<b>8. Intelligence Assessments</b>		See NOTE 2, below

**NOTE 1:** The final report shall be marked with the highest level of any single portion. However, the report may warrant classification at a level higher than any of its individual constituent portions due to the compilation of information. Mark each portion of the document with its own classification, and mark the document and each page with the overall classification of the document due to compilation.

**NOTE 2:** If you cite intelligence assessments in your final report, ensure that you retain and carry forward all protective markings assigned by the originator. Intelligence information will almost always be derivatively classified.

**NOTE 3:** The front cover of each report containing FOUO information must be marked as follows:

**This document contains information exempt from  
mandatory disclosure under the FOIA.  
Exemption 5 applies.**

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**L-8**  
**FOR OFFICIAL USE ONLY**

**ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPORD 01-01**

**REFERENCES: See Basic Order**

- 1. PURPOSE.** To provide Antiterrorism/Force Protection (AT/FP) policies and procedures regarding physical security, AT/FP vulnerability assessments, High-Risk Personnel protective measures, and AT/FP training requirements.
- 2. APPLICABILITY.** This Annex applies to all DoD elements and personnel operating in the USEUCOM under the security responsibility of USCINCEUR.
- 3. POLICY.** It is the policy of USCINCEUR to deter terrorism through the use of all reasonable means. While reducing the risk to USEUCOM personnel from acts of terrorism is a command responsibility, each person in the USEUCOM AOR must exercise proper caution and prudent judgment to reduce his or her vulnerability. Each USEUCOM activity (Service component command forces, Direct Reporting Units (DRU), Task Forces (TF), Joint Task Forces (JTF), and certain DoD personnel in Combined Task Forces (CTF) and multi-national organizations) must establish an AT/FP program within the guidelines of this order tailored to the mission and local conditions.

**4. AT/FP VULNERABILITY ASSESSMENT (VA) RESPONSIBILITIES**

**a. HQ USEUCOM ECSM**

**(1)** Oversee and direct the vulnerability assessment (VA) process for the USEUCOM AOR. Ensure USCINCEUR standards satisfy all Service and DoD requirements. Coordinate all VA issues between Services and Defense Agencies. See also Annex M, Appendix 2.

**(2)** Develop a prioritized master plan and schedule for VAs of all DoD sites and activities in the USEUCOM AOR. Give priority to those installations/activities supporting operational missions, (e.g. Task Force Falcon, Task Force Eagle, etc.) and/or high risk locations. Ensure VAs are conducted of all major Service component command facilities, installations, operating areas, other agencies/facilities/installations as per Annex M, Appendix 2. Monitor Service component command programs for VAs of their subordinate commands. Assess each Service component command's AT/FP program at least once every three years.

**(3)** Ensure all VA teams use applicable DoD and USEUCOM force protection standards and procedures, and that all team reports satisfy minimum VA requirements.

**(4)** Ensure assessments are conducted of off-installation residential security assessments. See Standard 30 in Appendix 1 of this annex for more guidance.

## FOR OFFICIAL USE ONLY

(5) Assist the Joint Staff, Service components and Defense Agencies (e.g., DTRA, DoDEA, DLA, etc.) in planning and conducting VAs in support of the master VA process. Provide a liaison officer with non-HQ USEUCOM VA teams as appropriate.

(6) Provide oversight of the USEUCOM Vulnerability Assessment Management Program (VAMP). In coordination with ECJ6, ECSM created the VAMP, which is a database available on the SIPRNet to track the results of VAs. This password-protected database is available through the HQ USEUCOM Force Protection homepage of the SIPRNet. The VAMP provides commanders with an accurate and current picture of vulnerabilities and the status of action being taken to correct identified weaknesses. Database also allows for the prioritization of all AT/FP requirements in theater. See Annex M, Appendix 2, Tab A.

(7) Ensure subordinate commands input required VA results in the VAMP Database.

(8) Provide advice and expertise to Service component commands and Defense Agencies who are loading data in the VAMP.

(9) Monitor VA results, compiling requests for assistance from local commanders unable to implement measures recommended in VAs.

### **b. All USEUCOM activities/installations**

(1) Conduct VAs IAW USEUCOM Standard 26 in Annex M, Appendix 1 and the guidelines in Annex M, Appendix 2. In addition, all activities must include the off-post residences of DoD personnel and their family members in these assessments.

(2) Update the VAMP database as VAs of installations or activities occur, or as recommendations are implemented, or when there is a change in local threat level or Force Protection Condition.

(3) Whenever the threat level changes or a threat/force protection alert or advisory is issued, compare the current VA report and existing vulnerabilities with new threat information. Report any changes to status to USEUCOM ECSM through the appropriate Service component command, and update the VAMP database.

(4) Ensure all VAs give particular emphasis to assessing the vulnerability of personnel, installations, and facilities to terrorist use of WMD (chemical, biological, or radiological agents).

(5) Document the results of each VA. Units may use Service, component or locally generated checklists, or the checklists enclosed in this OPOD (Annex M, Appendix 2) to conduct VAs. In addition, DoD Handbook 2000.12-H, reference (h), contains a number of other checklists to aid in the conduct of a VA. NOTE: The

## FOR OFFICIAL USE ONLY

security measures provided in the checklists may not be applicable to all units or activities. However, these checklists can serve as a basis for establishing or updating AT/FP programs.

**c.** Deficiencies noted by subordinate commanders will be prioritized and forwarded for resolution through that Service component's chain of command as necessary. Component commands will inform HQ USEUCOM ECSM without delay if required Service support to correct deficiency is not validated, or is inadequate.

**d.** DoD elements and personnel under the security responsibility of the COM.

**(1)** Per DoDD 2000.12, reference (g), USCINCEUR is responsible to conduct security reviews of DoD elements and personnel under the security responsibility of the COM. If a review is determined to be necessary, HQ USEUCOM ECSM will normally conduct these reviews in coordination with the USDR and the RSO.

**(2)** The objective of a security review is to identify any disparities in security coverage.

**(3)** Areas of physical security (concerning DoD elements and personnel under the force protection responsibility of the COM) that fail to comply with OSPB standards or are disparate from DoD/USEUCOM standards should be identified to the RSO for corrective action. If this coordination fails to correct noted deficiencies, refer to Annex C, Appendix 4, "Resolution of a 'Conflict on Post'," **(NOTE: The term "Post" is a Department of State term which means an overseas diplomatic mission, e.g., embassy or consulate.)**

**e.** Commanders must ensure procedures are implemented and included in their respective AT/FP Plans for the timely follow-up of corrective measures associated with each VA or program review by a higher headquarters. This is particularly critical for combatant units who rotate to the USEUCOM AOR, occupying the same location as the departing unit. Requests for waivers, exceptions, and variances to the requirements in this appendix are discussed in Annex M, Appendix 1 and Annex D, Appendix 1.

**5. ANTITERRORISM BRIEFINGS.** See Annex C, Appendix 1 for required briefings and Annex M, Appendix 5 for available training.

## ACKNOWLEDGE

**JOSEPH W. RALSTON**  
General, USAF

**APPENDICES:**

1. USEUCOM Prescriptive AT/FP Program Standards
  - TAB A: Sample Request for Deviation
2. Vulnerability Assessments
  - TAB A: USEUCOM Vulnerability Assessment Management Program (VAMP)
  - TAB B: Component Command Assessment Checklist
3. High-Risk Personnel
  - TAB A: High-Risk Personnel Transportation Support
  - EXHIBIT 1: Sample Request for Authority to Use Government Transportation for Unofficial Travel
  - TAB B: High-Risk Personnel (HRP) Security Checklist
  - TAB C: Non-Tactical Armored Vehicle Program
  - EXHIBIT 1: Annual NTAV Reporting Format
  - TAB D: Evasive Driver Training for High-Risk Personnel
4. Firearms for Personal Protection
  - TAB A: Sample Request for Authority to Bear Firearms for Personnel Protection
5. Antiterrorism/Force Protection Training
6. Procedures for Screening and Handling Mail



**APPENDIX 1 (USEUCOM AT/FP PROGRAM STANDARDS) TO ANNEX M  
(PHYSICAL SECURITY) TO USCINCEUR AT/FP OPORD 01-01**

**REFERENCES: See Basic Order**

**1. PURPOSE.** To establish the USEUCOM prescriptive Antiterrorism/Force Protection (AT/FP) program standards. The USEUCOM prescriptive standards correlate to the DoD Antiterrorism Standards found in DoD Instruction 2000.16.

**2. APPLICABILITY.** The standards in this Appendix apply to all DoD elements in the USEUCOM AOR except those elements for whom the Chief of Mission (COM) has security responsibility. These standards will be applied by each Service Component Command, Direct Reporting Unit (DRU), Joint Task Force (JTF) and Task Force (TF). Additionally, these standards apply to U.S. elements and personnel assigned to Combined Task Forces (CTF) or international units/billets, all deployed or TDY elements in the USEUCOM AOR, and to other Non-CINC Assigned Forces designated by agreement between USCINCEUR and the appropriate Chief of Mission (COM) as not being under the authority of the COM for security and AT/FP support. Unless specifically stated otherwise, the term “commanders”, as used herein, refers to those individuals vested with command authority in the chain of command from the CINC down to the installation/site level for permanent and/or temporary operations.

**3. DEVIATIONS.** The inability to meet minimum DoD and USEUCOM AT/FP standards and requirements may result in a higher AT/FP program risk. Commanders constantly must weigh risks involved in complying with the requirements and standards contained in this order. All commanders accepting a higher risk and deviating from this OPORD must seek approval through their Service component headquarters. Commanders who report directly to HQ USEUCOM will seek approval for deviation requests directly from HQ USEUCOM.

**a.** Approval authority for deviations from the DoD AT standards contained in DoD Directive 2000.12 and DoD Instruction 2000.16 as specified in this OPORD is the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD SO/LIC). Requests for such deviations must be forwarded through the chain of command to HQ USEUCOM ECSM for review prior to forwarding to the Joint Staff. The HQ USEUCOM Chief of Staff will approve all deviations from USEUCOM-directed standards and requirements, which exceed and/or are more stringent than DOD standards.

**b.** It is anticipated that most deviations from new, emerging and more stringent requirements in recently published DoD directives/instructions will involve the Standard 28 criteria specified in Appendix 1 to Annex D. Commanders should use the definitions, guidance and format provided in that Appendix to prepare and process deviations to the Standards listed below.

## FOR OFFICIAL USE ONLY

**4. PRESCRIPTIVE STANDARDS.** All components and commanders for whom USCINCEUR has AT/FP responsibility shall comply with the requirements specified in the following standards:

**a. USEUCOM STANDARD 1: Antiterrorism and Force Protection Policy.**

Commanders at all levels are responsible for the implementation of DoD AT/FP policies within their organizations. Component commanders must develop policies to ensure subordinate commanders comply with established requirements.

**b. USEUCOM STANDARD 2: Development of AT/FP Program Standards.**

The AT/FP program standards contained in this Appendix are the baseline standards for USEUCOM. Commanders at all levels must tailor these standards to Service and site specific requirements, and may issue more stringent requirements to supplement the standards contained herein. As a minimum, component command programs must address the following areas:

- (1) Procedures to collect and analyze terrorist threat information, threat capabilities, and vulnerabilities to terrorist attacks.
- (2) Terrorism Threat Assessments, Risk Assessments, and AT/FP Plans to include Terrorist Incident Response and Terrorist Consequence Management measures.
- (3) Procedures to enhance AT/FP protection, which might include, but not limited to, training programs, awareness campaigns, and technology applications.
- (4) Procedures to identify AT/FP requirements and to program for resources necessary to meet security requirements.
- (5) Vulnerability Assessments and a process to address, track and mitigate vulnerabilities.
- (6) Construction standards to mitigate the effects of a terrorist attack and procedures to identify, address, and potentially mitigate construction vulnerabilities associated with facilities not meeting minimum construction standards identified in Standard 28; see paragraph 4bb, below, and Annex D, Appendix 1.

**c. USEUCOM STANDARD 3: Assignment of AT/FP Operational Responsibility.**

This OPORD takes precedence over all force protection policies or programs of any DOD Component deployed in the USEUCOM AOR, and not otherwise under the security responsibility of the Department of State. HQ USEUCOM will ensure operational authority and responsibility for AT/FP is assigned for all DoD elements and personnel in the theater. HQ USEUCOM will pursue Memoranda of Understanding/Memoranda of Agreement/Command Arrangements Agreements (MOU/MOA/CAA) with COMs, other CINCs, and Defense Agencies to assign operational responsibility for

## FOR OFFICIAL USE ONLY

AT/FP in the USEUCOM AOR. HQ USEUCOM may assign a Service component and subordinate commanders operational responsibility for force protection over DoD personnel and elements who are not assigned, attached or OPCON to their command. Commanders at all levels must take appropriate measures to protect DoD personnel, families, facilities, and materiel to reduce the vulnerability and risk associated with terrorist use of Weapons of Mass Destruction (WMD). Commanders should resolve any conflicts regarding AT/FP responsibilities through the chain of command.

### **d. USEUCOM STANDARD 4: AT/FP Coordination in Overseas Locations.**

Commanders at all levels shall coordinate AT/FP efforts with host nation authorities and the appropriate COM commensurate with their level of authority using a MOU/MOA whenever possible. Commanders shall conduct coordination and liaison in accordance with guidance and security support arrangements in the DOS-DoD MOU on Force Protection On Security of DoD Elements and Personnel In Foreign Areas, reference (f), and applicable CINC-COM MOA. Intelligence and Counterintelligence elements shall coordinate their activities in support of AT/FP plans and programs through established procedures.

(1) USCINCEUR shall negotiate a CINC-COM MOA for all countries in the USEUCOM AOR to include the Russian Federation west of 100 degrees East.

(2) DoD elements not under the force protection responsibility of a geographic CINC, by law or under provisions of a CINC-COM MOA, shall comply with the State Department's Overseas Security Policy Board (OSPB) Security Standards.

(3) The Director of the Defense Intelligence Agency acting as DoD's executive agent for diplomatic security matters, through the United States Defense Representative (USDR), shall ensure that non-CINC assigned DoD elements, whose force protection responsibility rests with the COM, comply with OSPB standards.

(4) Disputes regarding AT/FP matters between DoD and DOS officials will be promptly reported to HQ USEUCOM ECSM. The "conflict resolution" process outlined in DoDD 5210.84, reference (r), should be followed, and every effort made to resolve the matter locally.

**e. USEUCOM STANDARD 5: AT/FP Program Development, Implementation and Assessment.** Commanders at all levels shall develop and implement a comprehensive AT/FP program to meet the requirements of this OPORD and at a minimum, the six specific areas identified in Standard 2. Additionally, AT/FP program elements will include threat assessments, planning, exercises, program reviews, training, and vulnerability assessments as well as a process, or sequence of reviews of the AT/FP program elements to continuously refine AT/FP Plans.

(1) Component commanders will designate, in writing, a staff officer to supervise, inspect, exercise, review, assess, and report on installation AT/FP programs

## FOR OFFICIAL USE ONLY

within their command. Component command programs must establish procedures to verify subordinate commands compliance with all requirements established in this OPOD.

(2) At the theater level, the HQ USEUCOM Special Assistant for Security Matters (ECSM) is the designated staff officer responsible for AT/FP program development, implementation and assessment.

(3) Another critical link to operating forces and potential vulnerability is logistics support. When it is necessary to contract logistics support, and that support could affect the security of operating forces, commanders at all levels will ensure that AT/FP measures are considered during the development of contracting requirements and the award process. Contracts should be structured to ensure AT/FP oversight is in place during the execution phase of the contract and a mechanism exists to identify AT/FP shortfalls in the evaluation process. Component commanders shall establish procedures with supporting contracting offices and agencies to verify that all logistics support contracts and agreements consider AT/FP for the particular security environment.

### **f. USEUCOM STANDARD 6: Assignment of Antiterrorism Officers (ATO).**

Commanders shall designate a commissioned officer, non-commissioned officer, or civilian staff officer in writing as the ATO for each installation or base, and deploying organization (e.g., battalion, squadron, ship) under their command. The designated ATO shall be trained in AT/FP procedures in a formal Service-approved Level II AT syllabus course. Component commanders must develop a process to verify units deploying into the AOR, or transiting through the AOR, have a trained, assigned ATO. See Appendix 5 to this Annex for criteria.

### **g. USEUCOM STANDARD 7: Application of DoD Terrorism Threat Analysis**

**Methodology.** The DoD Terrorism Threat Level classification system will be used to identify Terrorism Threat Levels in a specific country within the USEUCOM AOR. See Annex B, Appendix 2.

(1) The Department of Defense Terrorism Threat Level classification system is a set of standardized terms used to quantify the level of terrorism threat on a country-by-country basis. The Terrorism Threat Level terms are Low, Moderate, Significant, and High. The system evaluates the threat using a variety of analytical threat factors.

(2) Terrorism Threat Levels for each country in the USEUCOM AOR are set by DIA; however, USCINCEUR may set Terrorism Threat Levels for specific regions, personnel, family members, units, and installations based on more precise and focused intelligence reporting and analysis. Commanders at all levels shall use their own intelligence analysis (to include terrorist, criminal and other potential threats as well as the security environment of the host nation) as a tool in developing and updating plans and programs to protect assets within their command.

## FOR OFFICIAL USE ONLY

(3) Terrorism Threat Levels are estimates with no direct relationship to specific Force Protection Condition. A Force Protection Condition is a security posture promulgated by the commander in consideration of a variety of factors, e.g., mission requirements, terrorism threat analysis, Threat Level, risk assessment, etc. Terrorism Threat Levels should not be confused with Force Protection Conditions.

(4) Effective application of the Terrorism Threat Level classification system requires an integrated terrorism threat analysis, incorporating information collection from all sources. While Terrorism Threat Levels provide the basis for planning and programming AT/FP measures, Terrorism Warning Reports and current assessments are the “trip wires” for commanders to adjust security postures and implement increased AT/FP measures.

### **h. USEUCOM STANDARD 8: Threat Information Collection and Analysis.**

Identifying the threat is the first step and most critical element of an effective AT program and forms the basis for all planning considerations. Commanders at all levels shall task the appropriate organizations under their command to collect, analyze, and disseminate terrorist threat information. Collection efforts should exploit the full capabilities of law enforcement, security forces, intelligence, counterintelligence, and other available resources to report information of individuals, events and situations that could pose a threat to DoD personnel, families, facilities and resources. Commanders at all levels also should establish awareness programs and procedures to encourage all personnel under their command to properly report information on events or situations that could pose a threat to the security of DoD personnel, families, facilities and resources.

**i. USEUCOM STANDARD 9: Threat Information Flow.** Commanders at all levels shall develop a process to forward threat information throughout the chain of command to ensure maximum dissemination to all information pertaining to terrorist threat, or acts of terrorism involving DoD personnel or assets in the AOR. This notification system must include all DoD elements and personnel who may be impacted by the information and/or for whom the commander has AT/FP responsibility (e.g., non-CINC assigned forces in NATO billets or other geographically separated units as well as appropriate U.S. embassies).

(1) When notification to or coordination with an U.S. Embassy country team is required, the U.S. Defense Representative (USDR) will act as the USCINCEUR executive agent. Use guidance in Annex C, Appendix 2.

(2) When local information gaps exist, unit commanders should forward Requests for Information (RFI) via appropriate intelligence collection and production channels. (See Annex B and accompanying Appendices for more detailed guidance.) Transiting forces shall be provided with tailored terrorist threat information in accordance with the guidance in Annex E.

M-1-5

FOR OFFICIAL USE ONLY

**j. USEUCOM STANDARD 10: Potential Threat of Terrorist Use of Weapons of Mass Destruction (WMD).** Commanders at all levels shall take appropriate measures to protect DoD personnel, families, facilities, and materiel, and reduce the vulnerability to terrorist use of WMD. As a minimum, this shall include the development of estimates for potential terrorist use of WMD in their Area of Operation (AO). Threat assessments and collection plans should address the Essential Elements of Information (EEI) of the terrorist capability to acquire and use of WMD. Immediately report through the chain of command when significant information is obtained identifying organizations with WMD capabilities operating in the AO.

**k. USEUCOM STANDARD 11: Adjustment of Force Protection Conditions.** Commanders at all levels shall develop and document a process, based on terrorism threat information, mission requirements, and/or guidance from higher headquarters, to raise or lower Force Protection Conditions. All DoD installations, sites, facilities, and activities in the USEUCOM AOR shall comply with instructions in Annex C, Appendix 2, and Tab A thereto.

**l. USEUCOM STANDARD 12: Force Protection Condition Measures Implementation.** Commanders shall ensure that Force Protection Condition transition procedures and measures are properly disseminated and implemented within their AO. An At/FP Plan with a complete listing of site-specific AT measures, linked to a Force Protection Condition, will be classified, as a minimum, CONFIDENTIAL. When separated from the AT/FP Plan, specific AT measures and Force Protection Conditions remain FOR OFFICIAL USE ONLY (FOUO). All DoD installations, sites, facilities and activities in the USEUCOM AOR shall comply with instructions in Annex C, Appendix 2.

**m. USEUCOM STANDARD 13: Force Protection Condition Measures.** Commanders at all levels shall develop site-specific measures or action tasks for each Force Protection Condition using the security measures/actions required for each Force Protection Condition, per Annex C, Appendix 2, Tab A.

(1) Locally developed Force Protection Condition measures should be tailored to the environment and mission as well as being designed to counter the most probable threat. For example, a measure requiring securing buildings, rooms, etc. should be tailored to identify key facilities and the particular unit responsible for securing the areas.

(2) These measures will change, and generally become more stringent, as the threat situation increases from Force Protection Condition NORMAL to Force Protection Condition DELTA. For example, the same measure requiring buildings to be secured may specify five (5) key buildings to be secured during Force Protection Condition BRAVO, ten (10) during Force Protection Condition CHARLIE, and all facilities secured in Force Protection Condition DELTA.

## FOR OFFICIAL USE ONLY

(3) Whereas Terrorism Threat Levels are analytical assessments of terrorist activity in a country, or for specific regions, personnel, family members, units, and installations, Force Protection Conditions are graduated categories of measures or actions commanders take to protect personnel and assets from attack.

(4) Commanders at all levels may set a local Force Protection Condition. Subordinate commanders may raise a higher level commander's Force Protection Condition for their own area of operations. However, subordinate commanders shall not lower a higher level commander's Force Protection Condition, or deviate from the measures specified, without the higher level commander's concurrence. Commanders shall ensure proper notifications are made.

**n. USEUCOM STANDARD 14: Components and Commanders shall maintain a comprehensive AT Program for their AO.** Planning is critical to deterrence, detection, defense, and response to terrorist incidents. Where possible, Commanders may use existing plans to implement AT/FP programs; however, the installation AT/FP plan should be a "stand-alone" document, which incorporates or refers to existing plans. The Joint Staff (J-34) developed AT/FP Planning Template CD-ROM and WMD Template offer a useful guide to assist in developing local plans/OPORDs.

(1) The AT/FP Plan and supporting elements shall clearly describe site-specific AT measures. These directives shall be based on the guidance contained in this OPOrd and should be written from the Component level down to the installation level for permanent operations or locations, and incorporated in operations orders for temporary operations or exercises.

(2) At a minimum, AT/FP Plans and/or OPOrds shall address the following areas to provide a comprehensive program directive:

(a) **Terrorism Threat Assessment** (capability, vulnerability of facilities, criticality of facilities), to include WMD Threat Assessment.

(b) **Vulnerability Assessments**, to include associated countermeasures, installation priorities.

(c) **Risk Assessment** procedures to provide a means of making conscious and informed decisions to commit resources or enact policies or procedures which either mitigate the threat or accept the risk.

(d) **Terrorist Incident Response Measures** (determining scope of incidence, coordinated responses).

(e) **Terrorism Consequence Management Measures** (Command, Control, & Communications; mass casualty response, local or HN emergency response support).

## FOR OFFICIAL USE ONLY

**(f) AT/FP Physical Security Measures**, to include application of security and law enforcement assets (Force Protection Conditions, mass notification, delay (barrier plan, sensors, fortifications), deny (response forces, on-call reaction forces, HN police force), and coordination procedures).

**(g) Random Antiterrorism Measures (RAM)** implementation procedures for each Force Protection Condition.

**(h) AT/FP Training and Exercise Guidelines** to ensure compliance with the criteria in Standard 19, below.

**(i) Scope and Applicability.** Plan must incorporate all DoD elements and personnel for whom installation/activity commander has force protection responsibility.

**(3)** All AT/FP programs shall include tenets of countersurveillance (CS), counterintelligence (CI), and other specialized skills as a matter of routine, and shall identify an appropriate organizational element as the focal point for such AT/FP operations. Commanders at all levels shall constantly strive to ensure that proactive techniques and assets can be incorporated to detect and deter terrorists. Component commanders shall incorporate CI/CS assets in support of in-transit forces, particularly at higher threat level areas.

**o. USEUCOM STANDARD 15: Terrorism Threat Assessment - Critical Element for an Adequate AT/FP Plan.** Commanders at all levels shall prepare a terrorism threat assessment for their AO. At the theater level, these assessments will be prepared by the USEUCOM Joint Analysis Center (JAC) Molesworth. Component commanders shall designate which subordinate commanders will prepare these terrorism threat assessments for their AO. This normally applies to installation commanders and above.

**(1)** Threat assessments shall be prepared at least annually and should identify the full range of known or estimated terrorist capabilities for use in conducting vulnerability assessments and planning countermeasures. The terrorism threat assessment is the tool that commanders use to arrive at a judgment of risk and consequences of terrorist attack. Commanders shall integrate threat information prepared by the intelligence community, technical information from security and engineering planners, and information from other sources to prepare their assessments. As a minimum, terrorism threat assessments should include liaison with host nation security authorities, U.S. embassy country teams when appropriate, logistic support contractors, and airfield/port authorities (where applicable).

**(2)** Commanders shall consider the factors of threat, criticality, and vulnerability of facilities, programs, and systems, as well as deterrence/response capabilities during the assessment process. Terrorism threat assessments, combined with the Terrorism



## FOR OFFICIAL USE ONLY

Threat Level, shall be the basis and justification for recommendations on AT enhancements, program/budget requests, and the establishment of Force Protection Conditions.

(3) In addition to the annual threat assessment used for AT/FP program planning, continuous analysis of threat information is required to support the threat warning process.

(4) **Risk Assessments.** Commanders at all levels shall conduct risk assessments to integrate threat and vulnerability assessment information in order to make conscious and informed decisions to commit resources or enact policies and procedures that either mitigate the threat or define acceptable level of risk. While conducting risk assessments, commanders shall consider and analyze, at a minimum, the following four elements:

(a) The terrorist threat.

(b) The criticality of the assets, or mission being considered.

(c) The vulnerability of facilities, programs and systems to terrorist attack.

(d) Capabilities to conduct activities to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident.

**p. USEUCOM STANDARD 16: AT Physical Security Measures - Critical Element for an Adequate AT/FP Plan.** AT Physical Security measures shall be considered, supported, and referenced within the AT/FP planning directive to ensure an integrated approach.

(1) Where there are multiple commanders at an installation, the Installation Commander is responsible for coordinating and integrating individual unit physical security plans and measures into the overarching AT/FP plan. Commanders must develop a physical security plan for personnel and facilities under their authority to include procedures to:

- Detect possible hostile intent, activities, or circumstances.
- Assess the potential threat.
- Delay any unauthorized activity, persons, or attempts.
- Deny access, capability, or opportunity to create a circumstance which could lead to the loss of life or damage to mission critical resources.
- Notify appropriate personnel to take action.

(2) AT/FP plans shall integrate facilities, equipment, trained personnel, and procedures into physical security measures as part of a comprehensive effort designed

M-1-9

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

to provide maximum AT/FP to personnel and assets. This is best accomplished through the development of a synchronized matrix that outlines who will do what, where, when, and how.

**(3)** All physical security measures must include procedures for the use of physical structures, physical security equipment, chemical, biological, or radiological detection and protection equipment, 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.

**q. USEUCOM STANDARD 17: Terrorist Incident Response Measures - Critical Element for an Adequate AT/FP Plan.** Installation and/or Afloat commanders shall prepare installation-wide and/or shipboard terrorist incident response measures. These measures shall include procedures for determining the nature and scope of post-incidence response, and steps to reconstitute the ability to perform its mission and provide an appropriate level of AT/FP.

**(1)** 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 operations underway at the time of the terrorist incident will have significant bearing on the scope, magnitude, and intensity of response.

**(2)** 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 coordinate their responses into an integrated plan. Coordination with host nation response forces is critical. Commanders should conduct frequent drills to familiarize all personnel with individual responsibilities during a potential emergency.

**(3)** As a part of Terrorist Incident Response planning, commanders are encouraged to develop a set of recognizable alarms for potential emergencies. Each alarm should have its own set of reactions and a means to immediately sound the alarm.

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

## FOR OFFICIAL USE ONLY

(5) Theater-wide incident response measures are addressed in separate classified USCINCEUR and component command planning documents in the 0300, 0400 and 4299 plans series.

**r. USEUCOM STANDARD 18: Terrorist Consequence Management Measures - Critical Element for an Adequate AT/FP Plan.** Commanders must include terrorist consequence management preparedness and response measures as an adjunct to the installation AT/FP planning directive.

(1) The Terrorist Consequence Management measures must include the Command, Control and Communication process for emergency response and disaster planning and/or preparedness to respond to a terrorist attack for installation and/or base engineering, logistics, medical, mass casualty response, transportation, personnel administration, and local and/or host nation support. In addition, special circumstances imposed by the nature of a terrorist attack may require broader analyses to include higher levels of authority or command. Terrorist use of WMD, or terrorist attacks on dignitaries while visiting DoD installations, will require immediate close coordination with higher command, host nation authorities and the COM.

(2) The Consequence Management 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/FP Plan. However, the AT/FP Plan must provide guidance or reference to the appropriate plan.

(3) Consequence Management planning considerations should include potential terrorist use of: CBR weapons; large scale conventional explosive devices; introduction of contaminants into the water supply or Heating, Ventilation, and Air Conditioning systems, or any other tactic which could result in a significant loss of life or high order of destruction of mission critical resources.

**s. USEUCOM STANDARD 19: AT/FP Training and Exercises - Critical Element for an Adequate AT/FP Plan.** Commanders (installation, ship, squadron, battalion-level and above) shall conduct field and staff training to exercise the entire AT/FP plan, annually.

(1) Exercises may consist of "table top" or "chalk talk" exercises, but must be developed to effectively evaluate each annex of the plan. Additionally, **commanders must field exercise the critical elements of the AT/FP plan (Standards 15-18, above) at least annually** in addition to any "table top" exercises.

(2) Exercises should include host nation and Allied forces to the greatest extent possible, and encompass duty and non-duty hours. Exercises must include all tenant activities and DOD elements for whom the commander has force protection responsibility. AT/FP exercises should be executed with the intent to identify shortfalls

## FOR OFFICIAL USE ONLY

impacting the protection of personnel and assets against terrorist assault and subsequent consequent management efforts.

(3) To realize incorporation of lessons learned, commanders should maintain exercise documentation for no less than one year. Documentation should include lessons learned and corrective actions.

(4) AT training, particularly pre-deployment training, shall be supported by measurable standards and include credible deterrence/response standards, tactics, techniques and procedures. AT training also shall include probably terrorist scenarios and hostile intent decision-making. AT training shall be incorporated into unit level training plans and pre-deployment exercises.

(5) Commanders (ship, squadron, battalion-level and above) shall ensure joint operations and/or exercises incorporate AT training and planning for forces involved.

**t. USEUCOM STANDARD 20: AT Program Review.** Commanders at all levels shall review their own AT/FP program and plans at least annually to ensure compliance with directives and facilitate AT/FP program enhancement. For the same purpose, Commanders at all levels shall likewise conduct a documented compliance review of the AT/FP program and plan of their immediate subordinates in the chain of command at least annually.

(1) While such reviews do not constitute a vulnerability assessment, they are intended to ensure compliance with all applicable AT/FP directives and standards. The checklist in Tab B, Appendix 2 of this Annex is provided as a guide although commanders may develop their own process to satisfy this standard.

(2) To ensure the design and implementation of physical security measures coincident with the AT/FP program are consistent with the local Terrorism Threat Level and current terrorist threat assessment, commanders shall review their AT/FP program and plan whenever the Terrorism Threat Level changes.

**u. USEUCOM STANDARD 21: General Requirements for AT/FP Training.** Commanders shall ensure all assigned personnel receive appropriate training to advance AT awareness. Individual records shall be updated to reflect AT training in accordance with Service policy and guidelines.

**v. USEUCOM STANDARD 22: Level I AT Awareness Training.** Commanders shall 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 shall offer Level I AT Awareness Training to contractors employed by the DoD, consistent with the terms and conditions specified in the contract.

## FOR OFFICIAL USE ONLY

(1) Individual security awareness and individual AT training are essential elements of an overall AT program. Each individual must be exposed at the earliest opportunity to share in the responsibility of ensuring alertness and the application of personal protection measures.

(2) Commanders shall ensure all DoD personnel and their family members deploying/traveling on official government orders to and within the USEUCOM AOR receive Level I AT Awareness training and other antiterrorism training as may be required by Table M-5-1, Appendix 5, Annex M. DoD personnel deploying OCONUS, or to another area within the AOR where the terrorist threat and circumstances are significantly different, should be provided an AOR Update within three (3) months prior to travel in accordance with the guidelines specified in Standard 23, below.

(3) Level I AT Awareness Training shall be provided to all DoD personnel annually. Document such training in accordance with guidance in Standard 21, above.

(4) Family members traveling outside of the United States, its territories and possessions on official business (i.e., on an accompanied permanent change of station move) should have received this training as part of their pre-departure requirements. Family members to include those 14 years and older (or younger at the discretion of the DoD sponsor) traveling beyond CONUS on official business should receive Level I AT Awareness Training as part of their pre-departure requirements. Commanders will make this training available to family members who did not receive this training prior to their deployment to this AOR. Furthermore, the commander should encourage family members to receive Level I AT Awareness Training prior to any unofficial OCONUS travel, i.e., leave.

(5) Individuals may become qualified to administer Level I AT Awareness Training via two methods:

(a) Attending a formal service-approved Level II ATO Training course of instruction. Such training must review current AT publications and identify methods for obtaining AOR-specific terrorism threat analyses, updates, and warnings.

(b) Commanders may qualify individuals who are subject matter experts and have received formal training in AT and individual protection (e.g., military and/or security police, special agents, etc., who have received specific formal training in AT tactics, techniques, and procedures). These individuals may be individually exempted by the commander from the Level II ATO Training outlined in Table M-5-1 only if they receive additional training that reviews current AT publications and identifies the methods for obtaining AOR-specific updates.

**w. USEUCOM STANDARD 23: AOR Specific Training Requirements for all DoD Personnel.** Individuals traveling outside the United States, its territories and

## FOR OFFICIAL USE ONLY

possessions for either permanent or temporary duty shall complete the prescribed general AT/FP awareness training and AOR Specific Training prior to travel.

(1) DoD Service Components, Defense Agencies and functional CINCs are responsible to ensure that their assigned/attached personnel departing to the USEUCOM AOR are exposed to and execute the requirements in this OPORD, and have been provided AOR-specific information on ATFP protection. Individuals traveling to the USEUCOM AOR for either permanent or temporary duty shall have completed annual Level I AT Awareness Training and shall have received a specific AOR Update within three (3) months prior to travel.

(2) USEUCOM AOR specific AT/FP information is available to the Military Departments, supporting CINCs, Defense Agencies and Field Activities to support this required training. This information is available:

**Table M-1-1. Sources of AOR-Specific Training Information**

• In Annex C, Appendix 1, Tab A
• In Theater Clearance Guides
• Via SIPRNET at: <a href="http://www.eucom.smil.mil">http://www.eucom.smil.mil</a> . Follow link to Force Protection.
• Via SIPRNET at: <a href="http://www.ismc.sgov.gov/">http://www.ismc.sgov.gov/</a>
• Via SIPRNET at: <a href="http://www.jac.eucom.smil.mil/">http://www.jac.eucom.smil.mil/</a>
• Via INTERNET at: <a href="http://www.eucom.mil/hq/ecsm/tng.htm">http://www.eucom.mil/hq/ecsm/tng.htm</a>

(3) Component commanders and other authorities coordinating intra-theater movements of transiting units shall direct the parent commands attention to the requirements specified in paragraph 4w(1), above, and the information sources listed in paragraph 4w(2), above.

(4) Commanders at all levels who receive individuals who did not receive this training prior to departure from their last assignment shall report the deficiency through the chain of command. Service component commands will report this data to their parent Service and to HQ USEUCOM ECSM as directed on a semi-annual basis.

(5) Theater clearance authorities will not grant travel authority unless Level I AT Awareness Training and AOR-specific training has been verified/accomplished prior to departure from home station to the USEUCOM AOR. Upon request, the gaining command will assist in providing country-specific AT/FP information.

### **x. USEUCOM STANDARD 24: Level II AT Officer (ATO) Training.**

(1) Level II ATO training is designed to produce an AT advisor to the commander. Component commanders shall ensure that each installation and/or deploying unit (e.g., battalion, squadron, ship) is assigned at least one Level II ATO trained individual. HQ USEUCOM periodically conducts an AT/FP Program Managers and Security Engineering course, which focuses on AT/FP program management, but

## FOR OFFICIAL USE ONLY

this course does not satisfy the Level II ATO training requirements specified by DoD. Nevertheless, commanders are encouraged to send AT/FP functional managers to the USEUCOM course if scheduling permits. Coordination should be affected to arrange attendance by contacting HQ USEUCOM ECSM.

(2) Level III Pre-Command AT Training. Level III Pre-Command AT Training is designed to expose the prospective commander to AT issues. Services and/or DoD Agencies shall ensure that pre-command training tracks provide Level III Pre-Command AT Training to prospective commanders.

(3) Level IV AT Executive Seminar. The Level IV AT Executive Seminar is designed to expose senior Officers in the grades of O6-O8 and Department of Defense civilians in equivalent grades to AT issues. To arrange attendance to Level IV AT Executive Seminars, Components and Commanders should contact HQ USEUCOM ECSM. See Table M-5-1, Appendix 5, Annex M for criteria regarding Level I, II and III AT training.

**y. USEUCOM STANDARD 25: Training for High-Risk Personnel and High-Risk Billets.** CINCs have been given substantial AT responsibilities for Department of Defense personnel in their AORs assigned to high-risk billets or as personnel at high risk to terrorist attack. High Risk personnel (HRP) are eligible for advanced AT training. In some instances, this training may be extended to include family members.

(1) Commanders shall recommend the designation of individuals as being at high risk to terrorist attack and/or personnel assigned to high-risk billets. 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 Service Component Commander level, or in the case of DoD personnel/positions not assigned to a component command, DCINCEUR will retain this authority. However, for personnel visiting the USEUCOM 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. See Annex M, Appendix 3 for additional details and specific criteria for HRP designations.

(2) Commanders will forward a listing of high risk personnel and billets to HQ USEUCOM ECSM as directed annually and provide updates as changes occur. These lists will be consolidated and forwarded to the Service AT authority to enable the scheduling of requisite training.

(3) Whenever possible, this appropriate AT training should be conducted by the Services prior to arrival in theater.

**z. USEUCOM STANDARD 26: Vulnerability Assessments of Installations.** AT/FP vulnerability assessments provide a vulnerability-based analysis of an activity's

## FOR OFFICIAL USE ONLY

AT/FP program. The assessment identifies for the commander vulnerabilities that may be exploited by terrorists and suggests options that may eliminate or mitigate those vulnerabilities. Information derived from vulnerability assessments will be classified in accordance with the Defense Threat Reduction Agency (DTRA) Security Classification Guide and Annex L of this Order.

**(1) Assessment Focus.** Vulnerability Assessments shall focus on the assessed unit's overarching AT/FP program. These programs should be subject to continual assessment to avoid complacency and to gain benefit from experience from other assessments. Evolving terrorism threats, changes in security technology, development and implementation of alternative concepts of peacetime operations, and changing local conditions make periodic assessments essential. Vulnerability assessments will normally occur at the installation commander level and above. These assessments should consider the range of identified and projected terrorism threats against a specific location or installation personnel, facilities and other assets. The assessment should identify vulnerabilities and solutions for enhanced protection of DoD personnel and resources.

**(2) Local Vulnerability Assessments.** Component commanders will verify that local commanders conduct an annual vulnerability assessment of all facilities, installations, and operating areas within their area of responsibility. These local assessments must include all activities and elements residing as tenants on installations, or geographically separated but under the TACON of the local commander for AT/FP, as defined in the CINC-COM MAO and accompanying matrix. The assessment should identify vulnerabilities, determine the effectiveness of countermeasures, and adequacy of programming actions. The assessment should include, at a minimum:

- Validating and updating the local treat assessment.
- Reviewing AT/FP Plans (focusing on compliance with Standards 15-19; coordination with tasked agencies; availability of resources to execute the plan; and site-specific measures).
- Determining the effectiveness of AT/FP training programs.
- Assessing the physical security of mission critical resources and facilities.
- Analyzing the threat information collection and dissemination process.
- Identifying any shortfalls which preclude or limit execution of the AT/FP Plan.

**(3) Higher Headquarters Vulnerability Assessments (HHQ VA).** Commanders shall coordinate with their component command AT/FP office to schedule HHQ VAs of their activity in accordance with the established frequency cycle and procedures specified in paragraph 4z(4), below.

**(a)** HQ USEUCOM ECSM will track HHQ VAs to ensure compliance with this standard throughout the AOR; therefore, component command AT/FP offices must coordinate all HHQ VAs (Service, Defense Agency, MAJCOM, MACOM) with ECSM.



## FOR OFFICIAL USE ONLY

Based upon component inputs, ECSM will coordinate with the Joint Staff to schedule Defense Threat Reduction Agency (DTRA) teams to conduct Joint Staff Integrated Vulnerability Assessments (JSIVA) as well as the scheduling of any required out-of-cycle HHQ VAs.

**(b)** HHQ VAs must include all tenant activities and/or other DoD elements for whom the assessed installation/activity has AT/FP responsibility; this does not imply that each of these activities must be physically examined, but a sufficient review should be made to ensure that all activities are integrated into the installation's overall AT/FP program and plan. These assessments must focus on the most probable terrorist threat to an activity and appropriate countermeasures. In cases where no identified threat exists, the assessment should focus on the ability of activities to implement AT/FP measures under heightened Force Protection Conditions in response to an increased terrorist threat.

**(c)** To provide essential visibility, commanders shall prioritize, track, and report vulnerabilities identified during HHQ VAs to the next General Officer/Flag Officer or equivalent in the chain of command.

**(4) Assessment Scope and Frequency.** For installations shared with other CINCs and/or Services and/or Defense Agencies, one HHQ VA of the installation satisfies the frequency requirement for subordinate commands and/or tenants and/or detachments co-located within the confines of the assessed installation, or geographically separated but included in the HHQ VA. Additionally, HHQ VAs satisfy the annual requirement for a local VA.

**(a)** The following criteria will be used to schedule HHQ VAs of activities within the USEUCOM AOR:

**Table M-1-2. Assessment Frequency**

<b>TERRORISM THREAT LEVEL/ROTATION</b>	<b>ASSESSMENT TIME TABLE</b>
Deployed/High Turn-Over	At least annually
Significant/High Threat Areas	At least every 24 Months
Low/Moderate Threat Areas	Not to exceed 3 years

**(b)** Lowering the Terrorism Threat Level generally will not impact any scheduled HHQ VAs from authorities outside of USEUCOM (e.g., Service, Defense Agency, etc.), although HHQ assessments from authorities within USEUCOM and subsequent HHQ VAs by outside authorities may be scheduled based on the lower Threat Level. Increases in the Terrorism Threat Level will not necessarily affect the levels of frequency specified above unless the change has been in effect for 90 days or longer. If the Terrorism Threat Level increases from Moderate to Significant, or Significant to High, the requirement to schedule a HHQ VA to meet the 24 month criteria is effective from the time that the increased Terrorism Threat Level was declared.

## FOR OFFICIAL USE ONLY

(c) A HHQ VA will satisfy the requirement for an annual Local VA, except for those installations with deployed forces that require an annual HHQ VA. These deployed units (generally TFs or JTFs) are required both a local and HHQ VA on an annual basis.

**(5) AT/FP Site Criteria.** HHQ VAs shall be conducted at DoD components, housing areas, facilities, and/or activities at locations and command levels identified as "installations." For the purposes of this OPOrd, an assessment-eligible installation is:

- Any Department of Defense facility consisting of 300 or more personnel on a daily basis; and
- Any Department of Defense facility bearing responsibility for emergency response and physical security plans and programs; and
- Any Department of Defense facility possessing authority to interact with local non-military or host nation agencies or having agreements with other agencies or host nation agencies to procure these services.

**NOTE:** Notwithstanding the above, HHQ VAs may be conducted at any DoD component activity when HQ USEUCOM, or the responsible component command Headquarters and/or Defense Agency, identifies a time critical requirement or emergent need. All such out-of-cycle assessments will be coordinated with HQ USEUCOM ECSM prior to conducting the assessment.

**(6) AT/FP HHQ VA Functional Areas.** AT/FP HHQ VAs shall assess, as a minimum, the following functional areas:

**Table M-1-3. Functional Areas to be Assessed**

<p><b>1. AT/FP Plans and Programs.</b> The assessment shall examine the assessed installation's AT/FP program and ability to accomplish appropriate standards contained in this OPOrd and/or applicable AT/FP standards established by the appropriate Service, Defense Agency, or component command.</p>
<p><b>2. Counterintelligence, Law Enforcement Liaison, and Intelligence Support.</b> The assessment shall focus on the installation's process to receive threat information and warnings from higher headquarters and local resources, actively collect information on the threat (when permitted and in accordance with applicable law and regulations), process that information to include local fusion and analysis, and develop a reasonably postulated threat statement of the activity. Further, the assessment will examine the ability to disseminate threat information to all DOD personnel for whom the commander has AT/FP responsibility, including subordinate commands, tenant organizations, assigned to or visiting DoD personnel (including military members, civilians, and contractor employees, and dependents), and how that process supports the implementation of appropriate force protection measures to protect military personnel, DoD civilians and family members.</p>
<p><b>3. AT Physical Security Measures.</b> The assessment shall determine the assessed</p>

## FOR OFFICIAL USE ONLY

unit's ability to protect personnel by detecting or deterring terrorists, and failing that, to protect by delaying or defending against acts of terrorism. Physical security techniques include procedural measures such as perimeter security, security force training, security surveys, medical surveillance for unnatural disease outbreaks, and armed response to warning or detection as well as physical security measures such as fences, lights, intrusion detection devices, access control systems, closed circuit television cameras, personnel and vehicle barriers, chemical, biological, and radiological agent detectors and filters, and other security systems. The assessment should also consider commercial-off-the-shelf AT technology enhancements and potential solutions for those circumstances where existing technology or procedural modifications do not provide satisfactory solutions.

**4. Vulnerability to a Threat and Terrorist Incident Response Measures.** The assessment shall examine the assessed unit's ability to determine its vulnerabilities to commonly used terrorist weapons and explosive devices, to include weapons of mass destruction. The assessment shall further examine the ability to provide structural or infrastructure protection against terrorist events. The ability to respond to a terrorist event, with emphasis on a mass casualty situation, shall also be examined.

**5. Vulnerability Assessments for Terrorist Use of WMD.** The assessment shall assess the vulnerability of installations, facilities, and personnel within their AOR to terrorist use of WMD, to include the potential use of chemical, biological, nuclear or radiological agents or any other tactic which could result in a significant loss of life or high order of destruction.

**6. Risk Assessment Process.** The assessment will validate the effectiveness of mechanisms in place to provide the commander a means of making conscious and informed decisions to commit resources and/or enact policies or procedures which mitigate the threat, or to accept the risk.

**7. AT/FP Planning Directives.** The assessment shall examine written plans and/or programs in the areas of counterintelligence, law enforcement liaison, intelligence support, security and post-incident response (the ability of the activity to respond to a terrorist incident, especially a mass casualty event, to include a disease outbreak caused by terrorist use of biological weapons).

**8. Threats and Countermeasures.** The assessment shall focus on the most probable terrorist threat for the facility and appropriate countermeasures. In cases where no identified threat exists, units shall be assessed on their ability to implement AT measures under increasing Force Protection Conditions in response to an increase in the Terrorism Threat Level or terrorist threat warning.

**9. External Support and Exercises.** The assessment shall examine the availability and adequacy of resources to support plans and execute agreements as written. The extent and frequency to which plans are exercised also shall be examined.

**10. External Support.** The assessment shall examine the degree to which plans complement one another and support the assessed unit's ability to identify changes in the terrorist threat, react to threat changes by implementing appropriate AT measures and provide an appropriate response should a terrorist event occur..

**11. Host Nation, Local Community, Inter-Service, and Tenant Support.** The assessment shall examine the level and adequacy of support available to the activity

FOR OFFICIAL USE ONLY

from the host nation, local community, and where appropriate, inter-service and tenant organizations to enhance force protection measures or respond to a terrorist incident

**12. Coordination and Support.** The assessment shall determine the integration and feasibility of plans with the host nation, local community and inter-service and tenant organizations to provide security, law enforcement, fire, medical and emergency response capability in reaction to a terrorist event with emphasis on mass casualty situations.

**13. Agreements.** The assessment shall determine the status of formal and informal agreements with supporting organizations via Memoranda of Understanding or Agreement, Inter-Service Support Agreements, Host Tenant Support Agreements, or other models. Informal agreements can include Memorandums for Record to document verbal agreements and should be described as much as possible in the installation AT/FP plan.

**14. Site-Specific Characteristics.** Site-specific circumstances may require assessment of additional functional areas. These additional requirements shall be as directed by the CINC, Service or Defense Agency creating the team and should be based on site-specific characteristics such as Terrorism Threat Level, terrorist characteristics, geography, and security environment. Coordinate all such requirements with HQ USEUCOM ECSM prior to the assessment.

**(7) Team Composition and Level of Expertise.** As a minimum, the level of expertise and team composition must support the assessment of the functional areas described above. Team membership for HHQ VAs shall have expertise in the following areas: physical security; civil, electrical, or structural engineering; special operations; operational readiness; law enforcement and medical operations; infrastructure; and intelligence/counterintelligence.

**(a)** In exceptional cases, commanders may be required to tailor team composition and scope of the assessment to meet unique requirements of a particular site, but must meet the intent of providing a comprehensive assessment.

**(b)** Specific size and certification of expertise shall be as directed by the CINC and/or Service and/or Defense Agency creating the team. However, team members must be functionally orientated and have experience in the assessment area to be considered for team membership.

**(c)** Based on site specific factors such as Terrorism Threat Level, terrorist characteristics, geography and security environment, assessment teams may be augmented by personnel with expertise in the areas of linguistics; chemical, biological, radiological weapons effects; AT technology; explosive ordnance disposal; special warfare; communications; information assurance or operations; and other specialties as determined by the CINC and/or Service and/or Defense Agency sponsoring the assessment.

## FOR OFFICIAL USE ONLY

(d) For additional details and standards regarding Vulnerability Assessments, see Annex M, Appendix 2.

### **aa. USEUCOM STANDARD 27: Pre-deployment AT/FP Vulnerability**

**Assessments.** Based on the mission, prior to deploying on an operation or exercise, the commander of the deploying unit shall ensure a pre-deployment AT/FP vulnerability assessment is conducted. Based upon the results, commanders shall direct AT/FP measures to reduce risk and vulnerabilities before, during and after the deployment. Detailed and specific guidance for pre-deployment AT/FP vulnerability assessments and security requirements for forces transiting the USEUCOM AOR are contained in Annex E of this Order.

(1) Commanders shall contact the headquarters responsible for the deployment AO to ascertain the terrorist threat, criminal threat, military threat, health hazards, and required pre-deployment training.

(2) If warranted, commanders faced with emergent AT/FP requirements prior to movement of forces should submit Combating Terrorism Readiness Initiative Funds (CbTRIF) requests through established channels to procure necessary materials or equipment for required protective measures.

(3) Assessments and the subsequent implementation of standards must occur in a timely manner, and should be incorporated in pre-deployment planning and training. Pre-deployment assessments should assist commanders in updating AOR specific training and in obtaining necessary physical security materials and equipment to implement protective measures.

### **bb. USEUCOM STANDARD 28: AT/FP Construction Considerations.**

Commanders shall adopt and adhere to common criteria and minimum construction standards, e.g., new construction, renovation, or rehabilitation, to mitigate AT/FP vulnerabilities and terrorist threats. See USEUCOM AT/FP Construction Design Standards, Annex D, Appendix 1.

**cc. USEUCOM STANDARD 29: Facility and Site Evaluation and/or Selection Criteria.** Commanders shall develop a prioritized list of AT/FP factors for site selection teams. Use these criteria to determine if facilities, either currently occupied or under consideration for occupancy by DoD personnel, can adequately protect occupants against terrorist attack. Circumstances may require the movement of DoD personnel or assets to facilities the U.S. Government has not previously used or surveyed. AT/FP standards shall be a primary consideration in evaluating the suitability of these facilities for use.

**dd. USEUCOM STANDARD 30: AT/FP Guidance For Off-Installation Housing.** Commanders shall ensure all DoD personnel assigned to Moderate, Significant or High Terrorism Threat Level areas and are living in off-installation quarters receive, as a

## FOR OFFICIAL USE ONLY

minimum, the following guidance for selecting private residences to mitigate 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/FP guidance is provided. Individuals should be required to obtain approval through the Housing Office prior to leasing or purchasing a residence.

(1) Table M-1-4, below, provides general criteria for selecting economy quarters for lease or purchase.

**Table M-1-4. Off-Installation Housing Checklist**

<b>Off-installation/post Housing Considerations for Moderate Terrorism Threat Level Areas:</b>	
1.	<input type="checkbox"/> Give preference to residences that maximize safety and security while minimizing the need for security upgrades.
2.	<input type="checkbox"/> For single family residences, preference should be given to those with a perimeter barrier, such as a wall or fence that deters access to the property.
3.	<input type="checkbox"/> Preference should be given to residences with off street parking, and ideally secured in some manner.
4.	<input type="checkbox"/> Entrance areas and apartment hallways should be illuminated.
5.	<input type="checkbox"/> Entrances should have a substantial door.
6.	<input type="checkbox"/> Each entrance should have a capability to permit the occupant to identify visitors without opening the door.
7.	<input type="checkbox"/> Each entrance should have a deadbolt lock. A double cylinder lock should be used if placed within 40 inches of a glass side light or door window; fire safety rules should be considered when installing this type of lock.
8.	<input type="checkbox"/> Accessible window/openings should have a latching or locking mechanism.
9.	<input type="checkbox"/> Shatter resistant film should be considered for windows and doors vulnerable to explosive attack.
<b>Significant and High Threat Level Areas will also include the following (optional at lower threat levels):</b>	
1.	<input type="checkbox"/> Residences having multiple access routes to arterial roads should be given preference.
2.	<input type="checkbox"/> Grounds adjacent to the building facade and all entrance areas & apartment hallways should be illuminated.
3.	<input type="checkbox"/> Grills deemed adequate for local conditions are required on all accessible ground floor windows/openings where patterns of violence commonly use forced entry. Existing window barriers such as roll-down or hinged shutters or alarmed openings can preclude the need for grills.
4.	<input type="checkbox"/> Grilled residences above the fourth floor require a secondary means of escape.
5.	<input type="checkbox"/> Residences should be alarmed to protect accessible window/openings and doors.
6.	<input type="checkbox"/> A safe haven should be considered where the threat includes forced entry into residences accompanied by physical harm to an occupant—residences above the first floor are excluded.

(2) Commanders in Significant and High Terrorism Threat Level areas shall conduct periodic physical security reviews of off-installation residences for permanently assigned and temporary-duty DoD personnel. Such reviews shall use the same

M-1-22

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

terrorism threat, risk, and vulnerability criteria as that used to assess the safety and security of occupants of other facilities or installations housing DoD personnel on installations within the AOR. Based on the review results, Commanders shall provide AT recommendations to residents and facility owners, facilitate additional mitigating measures, and, as appropriate, recommend to appropriate authorities the construction or lease of housing in safer areas off the installation, or movement of personnel to facilities on an installation.

(3) Proper selection of off-installation housing sites can reduce personnel threat exposure. In Significant or High Threat areas, commanders shall ensure the completion of informal residential security reviews prior to personnel entering into formal contract negotiations for the lease or purchase of off-installation housing. The off-installation review should use the same terrorism threat, risk, and vulnerability criteria as that used to assess the safety and security of occupants of other facilities or installations housing DoD personnel on installations in the AOR.

(4) The intent of this standard is to enhance the safety, security, and awareness of DoD personnel by providing physical security assessments of off-base residences. Active involvement of commanders at all levels in the chain is required, particularly the individual's local unit commander/activity chief to ensure the requirements are met—the assessment of privately owned or leased (economy) quarters does not have to be conducted by a physical security expert. Anyone with proper training (and a checklist similar to that in Table M-1-4, above) can conduct this assessment for private (economy) residences.

(5) 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/FP 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/FP planning to react to changes to the Terrorism Threat Level.

(6) Commanders at all levels should incorporate family member and dependent vulnerabilities into all antiterrorism assessment, mitigation, and reporting tools. In Moderate, Significant, or High Terrorism Threat Level areas, commanders shall include coverage of facilities (e.g., DoD schools and daycare centers) and transportation services and routes (e.g., bus routes) used by DoD employees and their dependents.

**ee. USEUCOM STANDARD 31: Executive Protection and High Risk Personnel Security.** Commanders shall be familiar with treaty, statutory, policy, regulatory, and local constraints on the application of supplemental security measures for certain high-ranking DoD officials who are entitled to additional protection as a result of his or her position. Commanders shall take measures necessary to provide appropriate protective services for such individuals in high-risk billets and high-risk personnel in their AO. See Annex M, Appendix 3 for additional details and specific criteria for HRP designations.

FOR OFFICIAL USE ONLY

(1) Commanders should ensure individuals requesting supplemental security measures are aware of constraints and understand their individual responsibilities in accepting additional security measures. Commanders should ensure individuals receiving supplemental security measures have completed required AT/FP training, are cleared for assignment to billets, facilities, or countries requiring such protection, and have been thoroughly briefed on the duties of protective service personnel.

(2) Commanders should review supplemental security needs within 30 days of a change in the Terrorism Threat Level assigned to an AOR containing high-risk billets or to which high-risk personnel have been assigned. Complete review and revalidation of protective services shall be accomplished at least annually.

**5. Administration.** Table M-1-5, below, associates the standards from this Appendix with the existing DoD O-2000.12-H. Using the Handbook should provide commanders sufficient guidance and assistance in implementing their programs.

**Table M-1-5. AT Standards & Associated Chapters/Appendices  
from DoD O-2000.12-H**

DoD Standard	Chapter and Number	Related Appendices
1. DoD AT Policy	Chapter 1	See also Ref (a)
2. Development of CINC and/or Service and/or DoD Agency AT Program standards	Chapter 2	
3. Assignment of AT Operational Responsibility	Chapter 2	See also Ref (a)
4. AT Coordination in Overseas Locations	Chapter 12-14	
5. Comprehensive AT Program Development, Implementation, and Assessment	Chapter 4-13, 15-16	2, 4, 8, 10
6. AT Officers (ATO) shall be assigned in writing at each installation or base, and deploying organization (e.g., battalion, squadron, ship)	Chapter 15	
7. Application of Department of Defense Terrorist Threat Analysis Methodology	Chapter 5	4
8. Threat Information Collection and Analysis	Chapter 5	2, 4, 8, 9, 10
9. Threat Information Flow	Chapter 5	
10. Potential Threat of Terrorist Use of Weapons of Mass Destruction	Chapter 20	



FOR OFFICIAL USE ONLY

11. Adjustment of Threat Conditions (FORCE PROTECTION CONDITION)	Chapter 6	4
12. Force Protection Condition Measures Implementation	Chapter 6	4
13. Force Protection Condition Measures	Chapter 6	4, 11, 14, 15, 16
14. Commanders shall maintain a comprehensive AT Program for their areas of responsibility	Chapter 2	22, 23
15. Terrorism Threat Assessment	Chapter 17	2, 4, 8, 9, 10
16. AT Physical Security Measures	Chapter 7	2, 4, 22, 23
17. Terrorism Incident Response Measures	Chapter 17	4, 20, 22, 23
18. Terrorist Consequence Management Measures	Chapter 17	2
19. Training and Exercises	Chapter 20	2
20. AT Program Review	Chapter 2	
21. General Requirements for AT Training	Chapter 15	
22. Level I AT Awareness Training	Chapter 15	
23. AOR-Specific Training Requirements	Chapter 15	
24. Level II AT Officer Training	Chapter 15	
25. Training for High Risk Personnel and High Risk Billets	Chapter 13, 15	6, 11, 14, 15, 16, 17
26. Vulnerability Assessments of Installations	Chapter 9, 16	
27. Pre-deployment AT Vulnerability Assessment	Chapter 16, 19	19
28. AT/FP Construction Considerations	Chapter 9	2
29. Facility and Site Evaluation and/or Selection Criteria	Chapter 10	2
30. AT Guidance for Off-Installation Housing	Chapter 11	2, 16, 17
31. Executive Protection and Protective Services	Chapter 13	14, 19

FOR OFFICIAL USE ONLY

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
**General, USAF**

M-1-26  
FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY****APPENDIX 2 (VULNERABILITY ASSESSMENTS (VA) AND PROGRAM REVIEWS)  
TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPORD 01-01****REFERENCES: See Basic Order**

**1. GENERAL.** All DoD elements and personnel under the security responsibility of USCINCEUR shall be assessed to determine their vulnerabilities using the guidelines and criteria in Annex M, Appendix 1 and this Appendix. **These criteria are** in addition to any standards promulgated by their higher headquarters (HHQ), Command, or CINC that constitute their chain of command. In the event of a conflict between standards, the USEUCOM standards will override the conflicting Command's standards IAW DoDD 2000.12 and DoDI 2000.16. Additionally, commanders at all levels shall conduct internal AT/FP program reviews as well as program reviews of their immediate subordinates in the chain of command. These AT/FP program reviews will be designed to determine compliance with DoD and USEUCOM AT/FP standards and will satisfy the requirements specified in Standard 20. Additionally, local commanders will conduct VAs using the guidelines provided in Standard 26, and arrange for higher headquarters' (HHQ) VAs to satisfy the frequency criteria specified in Standard 26, **Table M-1-2.**

**2. CONCEPT.** The intent of a HHQ VA is to assess an activity's overarching AT/FP program and to provide focused expertise to facilitate AT/FP enhancements. The intent of a local VA is to provide the installation/ activity a detailed, comprehensive assessment that identifies vulnerabilities at the earliest juncture; validates the local AT/FP plans by ensuring they are executable; and ensures all stove-piped organizations, either located on the installation or for whom the installation/activity has AT/FP responsibility, are integrated into the local AT/FP planning directive and are afforded the same level of AT/FP support as local CINC-assigned forces. Locally conducted VAs should provide the commander with all of the necessary data required to identify mission essential or vulnerable areas (MEVA) and to conduct mission risk assessments. Nothing precludes local commanders from combining the Standard 20 program review and Standard 26 VA as long as both program objectives are achieved.

**3. ASSESSMENT CRITERIA.** Local VAs must be a comprehensive review addressing the broad range of physical threats to all mission critical areas (activities, facilities, resources) and **primary gathering facilities** as defined in Annex D, Appendix 1. HHQ VAs are not required to physically assess every single activity on the installation, but instead must assess an appropriate number to confirm the effectiveness of AT/FP procedures which are in place for the entire installation, site, or activity. Additionally, off-installation housing should be incorporated in the assessments process using the guidance provided in Standard 30.

**4. ASSESSMENT TEAM COMPOSITION.** Though team composition may vary based on the type of activity or installation being assessed, the team must, as a minimum, assess the areas listed in USEUCOM AT/FP Program Standard 26.

**M-2-1****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

a. HHQ VA Teams usually should consist of a Team Chief, a **Physical Security and Law Enforcement** Specialist, an intelligence and/or CI specialist, a structural engineer, operations readiness specialist, and a terrorist targeting/options/penetration specialist (Red Team). Local VA Teams should mirror as closely as possible the same team composition, but local teams often may not have the level of expertise provided by the HHQ VA Team. Regardless of composition, all teams must have some expertise to address the following areas:

<input type="checkbox"/> Physical Security
<input type="checkbox"/> Civil, Electrical, or Structural engineering
<input type="checkbox"/> Special Operations
<input type="checkbox"/> Operational Readiness
<input type="checkbox"/> Law Enforcement and Security Force Operations
<input type="checkbox"/> Infrastructure
<input type="checkbox"/> Intelligence/Counterintelligence

NOTE: "Red Team" is defined as a collection of subject matter experts that will review operations/plans from the adversary perspective. Term also may be used in conjunction with opposing forces (OPFOR) to give realism to exercises.

b. Other functional experts may augment the VA team. Augmentation will depend on type of assessment required, the nature of the activity/installation mission, the Terrorism Threat Level, and the Force Protection Condition (FPCON). Assessments may require expertise in preventive medicine, linguistics, chemical/biological/radiological weapons effects, emerging AT/FP technology, explosive ordnance disposal, Information Operations (IO), special warfare, or other specialties as determined by the commander or directed by a HHQ.

c. Headquarters conducting HHQ VAs are responsible to direct the size and verify the expertise of team members. Members may have expertise in a given field by virtue of school training or hands-on experience.

d. The following functions provide an example of the usual required areas of expertise for assessment team members:

**(1) Team Chief.** Provides overall management, training, and performance of the vulnerability team members; finalizing the assessment team out-briefing; preparing the population dynamics and risk assessment.

**(2) Security and Law Enforcement Specialist(s).** Key responsibility - installation, facility, and personnel security and safety. Major functions to perform: Assess overall physical security, operations, and information security. Review plans, training, personnel security and safety. Assess perimeter defense, off-post residences (if required), High-Risk Personnel program. Assess relationship and support from local law enforcement and other security agencies both local and U.S. Assess access

**M-2-2**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

control to include sensors and intrusion devices. Assess overall security planning and responsiveness to threat assessments and prepared intelligence estimates. Assess perimeter defensive positions and vehicular/personnel barriers. Assess lighting, police security, and security response planning and force capability. If vulnerabilities are found, formulate and suggest mitigating measures and assist in their implementation.

**(3) Intelligence/CI Specialist.** Key responsibility - intelligence operations. Major functions include: evaluate the collection, analysis, and dissemination of threat information. Assess intelligence estimates and intelligence products in the inspected unit's AT/FP plans and orders. Assess links with host nation intelligence and the HHQ intelligence assets. (See also the Penetration Specialist tasks below.)

**(4) Engineer.** Ideally, the assessment team will include two engineers with different specialties and focus, but one engineer with some expertise in each area is acceptable.

**(a) Civil, Electrical or Structural Engineer.** Key responsibility - threat and damage assessment from terrorist weapons estimates; suggestions for threat protection or damage mitigation measures. Major functions to perform: Assess damage mechanisms including blast, shock, and fragmentation. Calculate hazardous radii based on structural dynamics and calculated structural loads. Assess building and barrier resistance or mitigation of threat weapons effects. Determine appropriate standoff distance, potential hardening or other mitigating measures. Assess systems related to physical security and personnel protection (warning devices, alarms, etc.). Assess/identify safe havens. Assess mechanical, electrical, and other service systems for vulnerability to weapons effects and suggest mitigating measures. If structural vulnerabilities are found, suggest measures to correct problems and assist in their implementation.

**(b) Infrastructure Engineer.** Key responsibilities include infrastructure security including mechanical, electrical, and other service systems; fire, safety, and damage control. Duties include: Assessing fire-protection systems, fire suppression, and fire alarms to determine their ability to facilitate evacuation, initiate a response, and extinguish fires resulting from a terrorist incident. Assessing the electric supply and distribution systems to determine if power will continue to be supplied to critical facilities during a terrorist incident. Assessing fuel storage and delivery to determine if they can be exploited by a terrorist to divert first responders and/or be a casualty multiplier. Assessing telecommunication facilities and distribution systems to determine vulnerabilities of critical nodes, which if lost could hinder an emergency response to a terrorist incident. Assessing the water supply and distribution systems to determine their vulnerability to waterborne contamination. Assessing heating, ventilating, and air-conditioning (HVAC) systems to determine vulnerability to WMD. Formulating and suggesting corrective measures.

**FOR OFFICIAL USE ONLY**

**(5) Operations Readiness Specialist.** Key responsibility - emergency medical and individual readiness assessment. Major functions to perform: Assess vulnerability of installation utilities and plans for back-up services. Assess disaster response plan including WMD response. Assess availability of support to include use of local national capabilities. Assess individual, personnel, facility, and installation protection capabilities. Assess emergency medical capabilities and planning including the identification of key assets and infrastructure. Assess recovery procedures and planning to understand the ability to recover from loss of key assets, infrastructure, or facilities. Assess planning/consideration of evacuation as a risk mitigating measure. If vulnerabilities are found, formulate and suggest mitigating measures and assist in their implementation.

**(6) Penetration Specialist (Red Force).** Key responsibility - performs logical analysis and prepares possible conclusions regarding terrorist targets and target vulnerabilities based on processed intelligence information, knowledge of terrorist capabilities and methods, and in view of U.S. installation, facility, and personnel safety and security practices. Develop possible threat scenarios. Assess installation, facility, and personnel vulnerability in view of scenarios, and in consideration of on-going counterintelligence activity, demonstrated capabilities in exercises, capabilities of local authorities, and terrorist intelligence activities. Propose additional security, counteraction, and threat reduction efforts. An intelligence or CI specialist may assess these areas.

**e. Other areas.** Assessments may evaluate other aspects of force protection. Among these include preventive medicine. If deployed, the preventive medical member must be qualified to evaluate the safety and vulnerability of local food and water sources, perform an epidemiological risk assessment, evaluate local medical capabilities, perform a vector/pest risk assessment, determine adequacy of hygiene of local billeting and public facilities, and perform an environmental risk assessment.

**5. ASSESSMENT PLANNING, PREPARATIONS AND CONDUCT.** This section provides an example of the activities an Assessment or Program Review Team may perform when preparing to provide an AT/FP assistance visit and upon completion of the field visit. The tasks include the site survey actions, and follow-on actions subsequent to the trip. The length of an assessment may vary based on the nature of the assessment. The example below is based on a five-day assessment schedule. For specific requirements associated with Joint Staff Integrated Vulnerability Assessments (JSIVA), see paragraph 6, below.

**a. Pre-assessment Preparations.** Schedule assessments at least 30 day prior to the visit to allow specific travel requirements, such as medical, visa, ticket cost minimization, and threat and site information, to be accommodated. The Assessment/Program Review Team should coordinate the particulars of the visit with the installation POC, including theater/country clearances.

**FOR OFFICIAL USE ONLY**

(1) The administrative/logistics preparations include any requirements for invitational travel orders, passports, visas, inoculations, insurance (health and life) and other legal issues, and emergency information forms. Preparations also include travel arrangements (tickets, lodging or billeting), travel kits (pharmaceuticals and supplies), equipment checkout and packaging/shipping.

(2) Security preparations include submitting requests for country/site clearances, identifying classified courier requirements, coordinating secure storage, identifying a security representative, presenting mandatory threat and security procedures briefing.

(3) The key element of preparation is the site folder development. The site folder is the official record of all assessment team information gathering, analysis, recommendations, and assistance for the installation commander. A critical aspect of the site folder formation is the intelligence information gathering relative to the terrorist threat.

(4) The team should obtain all intelligence on groups, motivation, intent, tactics, weapons activities and operating areas from DIA, JAC Molesworth, and other sources. Request in advance a complete list of activity/installation characteristics, including layouts, drawings, functions, personnel, and procedures be sent to the AT/FP assessment team or be made available upon arrival.

(5) Obtain a copy of the installation/activity's comprehensive AT/FP plan and any supporting plans or agreements at least 60 days in advance. Ensure all required/core assessment team members receive a copy of these documents and review them prior to the assessment. Additionally, as instructed by the commander directing the assessment, provide a copy of these documents to potential team members (supplemental members) such as medical; **chemical, biological, radiological and nuclear**; explosive ordnance disposal; communication; and information operations officers. These officers should review the plan from the standpoint of their functional expertise. They should make recommendations on the adequacy of the plan as it relates to their functional area, recommend any follow up action and questions for the assessment team, and if warranted recommend inclusion of additional functional experts on individual assessments. For example, if the command's medical officer does not believe identified concerns for a particular assessment can be adequately addressed by required/core team members, he or she should recommend inclusion of a component medical expert on the assessment team.

(a) When the assessment will be conducted by a Joint Staff Integrated Vulnerability Assessment (JSIVA) team, the component headquarters and ECSM will coordinate for the additional component functional expert to accompany the team. In order to accomplish this coordination, the component headquarters and ECSM must be officially informed of this request 30 days in advance of the JSIVA.

**FOR OFFICIAL USE ONLY**

**(b)** Observations or comments by the HQ USEUCOM or Component Command representatives regardless of functional area may be included in the JSIVA out-briefing or assessment report at the discretion of the JSIVA team chief. Regardless of the JSIVA team chief's decision on including such inputs in the official JSIVA documents, HQ USEUCOM and Component Command representatives should submit their observations through their chains of command for information and action as appropriate. Additionally, Component Commands shall ensure all AT/FP related observations are loaded into the USEUCOM Vulnerability Assessment Management Program (VAMP) within 10 duty days following the out-briefing of the results of the JSIVA visit.

**(6)** All assessment team members (core and supplemental) should be involved in the development and maintenance/updating of vulnerability assessment checklists.

**b. Conduct of the Assessment.** Upon arrival and check-in (badging and security), the team will provide an in-brief for the installation commander, staff, and designated technical point of contact. Site personnel will conduct a site familiarization briefing and tour for team members.

**(1)** Administrative activities include establishing the team support area, setting up equipment, scheduling team/technical POCs meetings and discussions, ensuring classified material control, establishing personnel locator, and organizing materials (viewgraph, photos, and diagrams) for the out-briefing and site folder. The program review team should use a checklist similar to the USEUCOM assessment checklist (see Tab B to this Appendix) that may incorporate Service-specific requirements to conduct its assessment. However, the team may also refer to the security checklists found either in **Tabs C and D** to this appendix or in the appendices of DoD Handbook 2000.12-H.

**(2)** The team leader should hold a coordination meeting at the end of each day to determine progress, develop out brief inputs, and address any issues. In the latter half of the fourth day of the assessment, the team leader should coordinate and finalize the out-brief with the technical POCs. The morning of the fifth day, the team leader should provide the activity commander and staff an out-brief. This will include the vulnerability assessment and improvement options.

**c. Post-assessment Activities.** Within 30 days of the visit conclusion, the assessment/program review team should forward a summary narrative report and annotated briefing to the activity visited. The activity commander shall evaluate the report and assign a color-coded indicator following the criteria listed in paragraph 7, below, and then further distribute the report. Commanders will forward a copy of the report to the appropriate component command headquarters NLT 10 duty days after assigning a color code indicator. Commanders can request follow-on assistance, to include technical characteristics of improvement options, cost estimates and generic sources of materials and equipment.



**FOR OFFICIAL USE ONLY**

**d.** Commanders will report the findings of assessment teams through inputs to the Vulnerability Assessment Management Program (VAMP) database. See Tab A to this Appendix. Given the nature of deficiencies reported, the responsible HHQs may determine a reassessment is required.

**e.** ECSM will receive electronic versions of the final JSIVA reports within 45 days after completion of the assessment. Upon receipt of this electronic version, ECSM will post the report onto the VAMP.

**f.** Examples of HHQ teams available to conduct assessments include: JSIVA teams, Service teams, HQ USEUCOM teams, and component command teams.

**6. JSIVA REQUIREMENTS.** The following process applies for all JSIVAs in USEUCOM:

**a.** Not later than 150 days to the scheduled JSIVA visit, the installation commander must submit a letter to HQ USEUCOM (ATTN: ECSM) through the appropriate component command headquarters certifying the AT/FP Plan is signed and executable. An executable plan:

**(1)** Has been approved and signed by the U.S. commander responsible for AT/FP.

**(2)** Has been exercised and can be executed by the installation commander with his/her own assets, or the assets that non-military/host nation or Allied forces have agreed to provide.

**(3)** Includes, at a minimum, the required elements identified in USEUCOM Standard 14: Threat Assessment; Vulnerability Assessments; Risk Assessment; Incident Response Measures; Consequence Management Measures; Physical Security Measures; Random Antiterrorism Measures (RAM); Training and Exercise Guidelines; and Scope includes all appropriate personnel and facilities.

**b.** If the installation has had a previous JSIVA, the installation commander must identify what actions the unit has taken to address the previously identified vulnerabilities. Actions might include procedural changes, programmatic actions or commander's risk assessment decisions. This information should be provided in a message to arrive at the Defense Threat Reduction Agency (DTRA) with copies to HQ USEUCOM ECSM and the appropriate component command headquarters NLT 60 days prior to the scheduled arrival of the JSIVA team.

**c.** All JSIVA team identified vulnerabilities must be entered into the USEUCOM VAMP NLT 10 duty days following the JSIVA out-brief.

**FOR OFFICIAL USE ONLY**

d. Following the receipt of the written JSIVA report, the installation commander must prioritize and track the vulnerabilities and concerns identified by the JSIVA team.

(1) Within 30 days of receipt of the JSIVA report, the local AT/FP office or respective component command headquarters must input all identified vulnerabilities and concerns into the USEUCOM VAMP. To maintain a record of actions and decisions, include all vulnerabilities/concerns identified by the JSIVA team even if they have been mitigated or determined to be an acceptable risk through the commander's risk assessment.

(2) Within 60 days after receipt of the JSIVA report, the commander must provide a written report of actions taken, or planned, to mitigate each of the vulnerabilities and concerns identified during the JSIVA. Commanders will provide the report in a message to the first General/Flag officer in the chain of command with information copies to HQ USEUCOM ECSM and the appropriate component command headquarters. Additional updates will be provided as necessary.

e. In addition to the reporting requirements in paragraph 6d, above, the following USEUCOM procedures will be applied when a JSIVA team identifies a repeat procedural vulnerability. (Note: a procedural vulnerability is one which can be mitigated by changing tactics, techniques or procedures at little or no cost.)

(1) Within 30 days after receipt of the final JSIVA report, the commander responsible for AT/FP must submit a documented course of action to mitigate the procedural vulnerability and an estimated completion date for each repeat procedural vulnerability identified by the JSIVA team. This report will be sent to HQ USEUCOM ECSM through the component command AT/FP office.

(2) Within 60 days after receipt of the final JSIVA report, the commander must certify the procedural vulnerability is corrected, or request a 30-day extension for HQ USEUCOM ECSM.

(3) Within 90 days after receipt of the final JSIVA report, ECSM and the component command AT/FP office will evaluate the corrective action. ECSM will conduct a staff assistance visit during this time if appropriate.

**7. CRITICAL PROGRAM REQUIREMENTS.** VAs provide commanders with a comprehensive picture of their AT/FP posture. VAs also provide USEUCOM and the component commands with the ability to identify and track AT/FP trends and deficiencies.

a. At a minimum, HHQ VAs will address all areas as described in USEUCOM AT/FP Program Standard 26, Table M-1-3 (see Annex M, Appendix 1).

**FOR OFFICIAL USE ONLY**

b. There are eight Critical Program Requirements which all installations and activities are expected to meet to satisfy the basic AT/FP program standards promulgated by DoD and USCINCEUR. The following Critical Program Requirements are the baseline to determine the overall installation/activity color-code rating:

<input type="checkbox"/> 1. Comprehensive AT/FP Program Established and Maintained. (Standards 2 and 14)
<input type="checkbox"/> 2. Trained AT Officer (ATO) Assigned in Writing. (Standards 6 and 24)
<input type="checkbox"/> 3. Local Threat Assessment Conducted Within Last 12 Months. (Standard 15)
<input type="checkbox"/> 4. Threat Information Notification System Established. (Standard 9)
<input type="checkbox"/> 5. Comprehensive Local Vulnerability Assessment and Program Review Completed Annually. (Standards 20 and 26)
<input type="checkbox"/> 6. Signed, executable AT/FP Plan Fully Coordinated with Tasked Units. (Standard 14)
<input type="checkbox"/> 7. AT/FP Plan Exercised Annually and Lessons Learned Documented. (Standard 19)
<input type="checkbox"/> 8. Countermeasures In Place to Mitigate Known Vulnerabilities. (Standard 14)

**8. COLOR-CODED RATINGS.** The following Color-coded Rating scheme will be used by HHQ and local VA teams to give visibility to serious program weaknesses and to facilitate the tracking of corrective actions:

a. Commanders must determine the baseline color-code rating using the Critical Program Requirements listed above. Failure to meet any of the Critical Program Requirement areas will result in an overall "RED" rating. A commander may assess the installation to be "AMBER" even if the activity or installation meets each of the eight Critical Program Requirements, but still has serious weaknesses. Forward final color-code ratings (and identified vulnerabilities/problems) through the chain of command using the USEUCOM VAMP. .

b. The color indicator code denotes an installation's/activity's overall assessment status:

(1) RED - Installation's/activity's AT/FP program does not meet the minimum USEUCOM AT/FP Program standards. .

(2) AMBER - Installation's/activity's AT/FP program meets the minimum USEUCOM AT/FP Program standards, but Commander determined program requires some improvements. .

(3) GREEN – Installation's/activity's AT/FP program meets, or exceeds, all USEUCOM AT/FP Program standards.

c. Those installations/activities assessed as RED will require a reassessment within 6 months after the original assessment. The appropriate HHQ will determine the type and scope of reassessment. If the vulnerabilities/problems identified cannot be corrected at the time of the reassessment, the appropriate HHQ will determine if a HHQ assessment is required for that location. Once the identified vulnerabilities/ problem

**M-2-9**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

areas have been corrected, commanders will reevaluate their installation's AT/FP readiness and assign a new color-coding.

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
**General, USAF**

**TABS:**

- A. USEUCOM Vulnerability Assessment Management Program (VAMP)
- B. Component Command Assessment Checklist
- C. Vulnerability Assessment Checklist
- D. Assessment/Survey Checklists

**FOR OFFICIAL USE ONLY****TAB A (VULNERABILITY ASSESSMENT MANAGEMENT PROGRAM) TO  
APPENDIX 2 (VULNERABILITY ASSESSMENTS) TO ANNEX M (PHYSICAL  
SECURITY) TO USCINCEUR AT/FP OPORD 01-01**

**1. GENERAL.** DoD Directive 2000.12 requires each geographical CINC to identify activities that do not meet force protection standards. The USEUCOM Vulnerability Assessment Management Program (VAMP) provides all authorized commanders the means to record and track installation/activity shortcomings, prioritize vulnerabilities and identify resource requirements.

**2. VULNERABILITY ASSESSMENT MANAGEMENT PROGRAM (VAMP)****a. The VAMP:**

(1) Provides a database to document Standard 26 vulnerability assessment findings, both higher headquarters (HHQ) and local.

(2) Documents a commander's risk assessment decision for each vulnerability.

(3) Tracks the status of known vulnerabilities until mitigated.

(4) Provides ability to prioritize antiterrorism/force protection (AT/FP) resource requirements and input into the Planning, Programming, and Budgeting System (PPBS).

(5) Provides commanders a vehicle to identify requirements to the responsible chain of command.

(6) Provides a ready reference to track the status of installations and activities by Force Protection Condition (FPCON) and/or Terrorism Threat Level.

**b.** The VAMP is accessible through the SIPRnet at the HQ USEUCOM Force Protection homepage, [http://www2.eucom.smil.mil/hq/ecsm/ecsm\\_home.htm](http://www2.eucom.smil.mil/hq/ecsm/ecsm_home.htm).

**3. CONCEPT OF OPERATIONS**

**a.** The Office of the Special Assistant for Security Matters (ECSM) manages the VAMP with assistance and expertise provided by HQ USEUCOM ECJ6. ECSM is responsible for designing and upgrading this system, providing passwords and write permissions, and conducting training as needed.

**b.** Component command AT/FP offices monitor the VAMP for accuracy and timely input of data. Component command AT/FP offices must validate the accuracy of the data in the VAMP and notify ECSM via email NLT the 3rd duty day of the month. Additionally, the component commands use the data to develop AT/FP funding priorities.

**M-2-A-1****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**c.** Installation Antiterrorism Officers (ATO) administer the VAMP by entering, editing, and maintaining accuracy of data. ATOs must validate the accuracy of VAMP data monthly and edit/update the VAMP:

**(1)** Upon completion of an assessment, either local or HHQ. NOTE: Installations must enter known vulnerabilities identified during a JSIVA NLT 10 duty days after the out-brief. Installations must input all other vulnerabilities identified by the JSIVA team NLT 30 days following receipt of the written report.

**(2)** Whenever the status of a vulnerability changes (e.g. vulnerability eliminated; project design status change; or project funded).

**(3)** As soon as possible after changing the FPCON.

**d.** VAMP access is controlled and limited to a “need to know” basis. Individuals with a need to establish a VAMP account must submit a request through their component command AT/FP office. Individuals not assigned to a specific component command should contact ECSM directly. The Special Assistant for Security Matters approves all requests for VAMP accounts, and ECSM validates accounts semi-annually. Components must notify ECSM when an authorized user no longer requires access to the VAMP. Individuals must provide the following information when establishing an account:

<b>Rank:</b>	<input type="text"/>	Input new user's rank. If civilian, enter <i>Civ</i> .
<b>First Name:</b>	<input type="text"/>	Input new user's first name.
<b>Last Name:</b>	<input type="text"/>	Input new user's last name.
<b>Command:</b>	<input type="text"/>	Enter user's duty command.
<b>Service:</b>	<input type="text" value="EUCOM"/>	Select user's service.
<b>Directorate:</b>	<input type="text"/>	Enter user's directorate.
<b>Email Address:</b>	<input type="text"/>	Enter user's email address.
<b>DSN Phone:</b>	<input type="text"/>	DSN phone number.
<b>Civilian Phone:</b>	<input type="text"/>	Enter a commercial phone number.

Figure M-1-A-1

M-2-A-2

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**4. Process.** VAMP is a user-friendly drop-down menu program. The next several pages display and describe each screen within VAMP. Additionally, the explanations provide mandatory guidance and helpful information to navigate through VAMP.

**a. Log on Procedures.** VAMP is a web-based program and authorized users can access VAMP from any SIPRnet terminal. To log on, users simply input username and password. VAMP will deny access after 3 attempts to enter with an incorrect username and/or password. If locked out, follow the directions provided by VAMP and call ECSM.

**b. VAMP Version 5.0 Main Screen.** After successful log on, VAMP displays this screen.

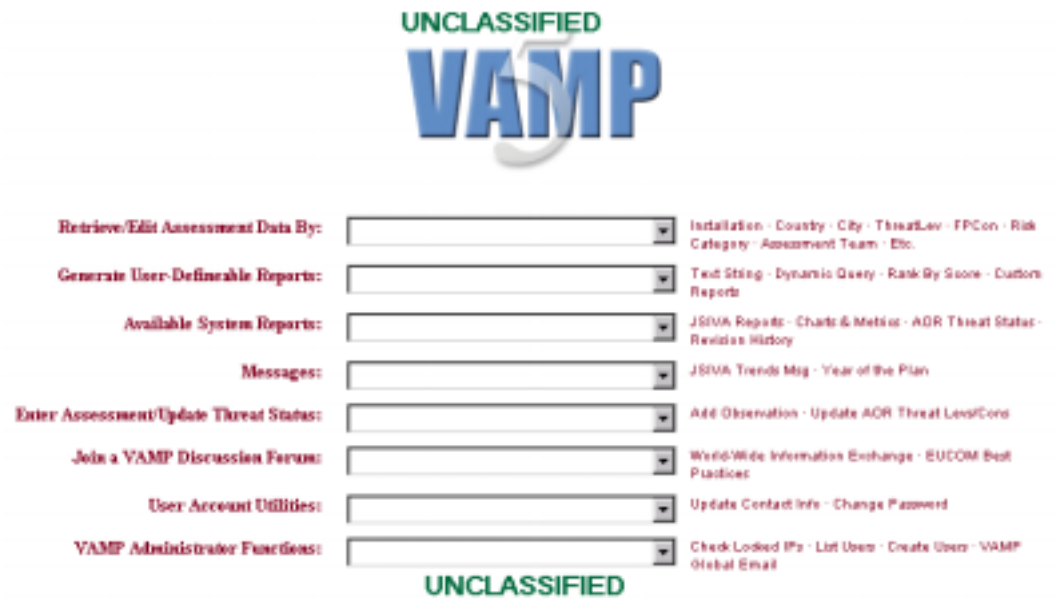


Figure M-1-A-2

**FOR OFFICIAL USE ONLY**

c. **Retrieve/Edit Assessment Data By.** Provides reports for:

(1) **Installation.** Access to assessment data by installation/activity. This is the starting point for editing, updating, or retrieving data only, NOT entering data. A user selects installation/activity through drop down menu.

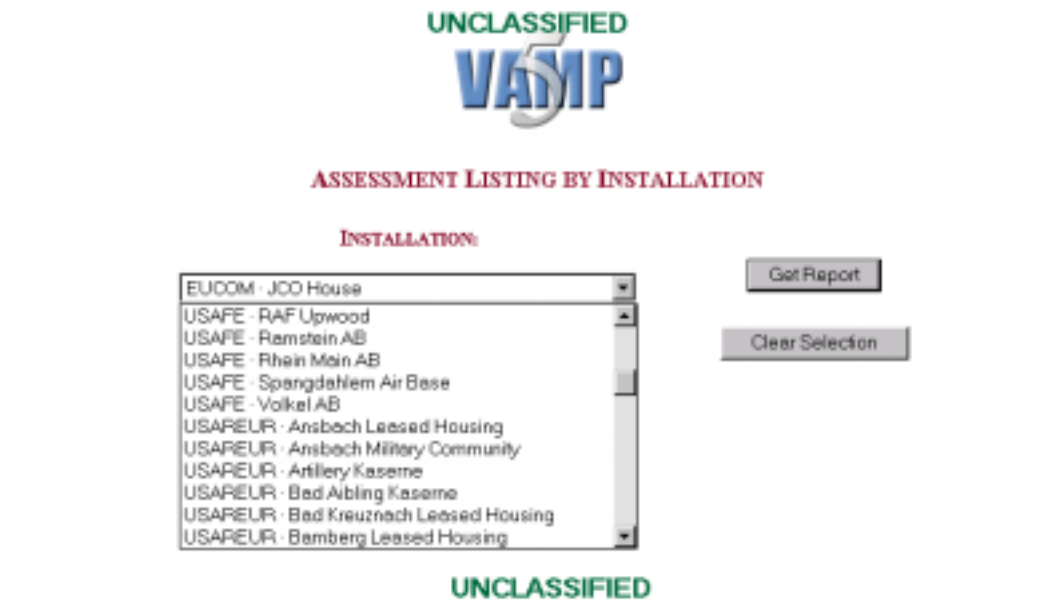


Figure M-1-A-3

(2) **Country.** Access assessment data by country.

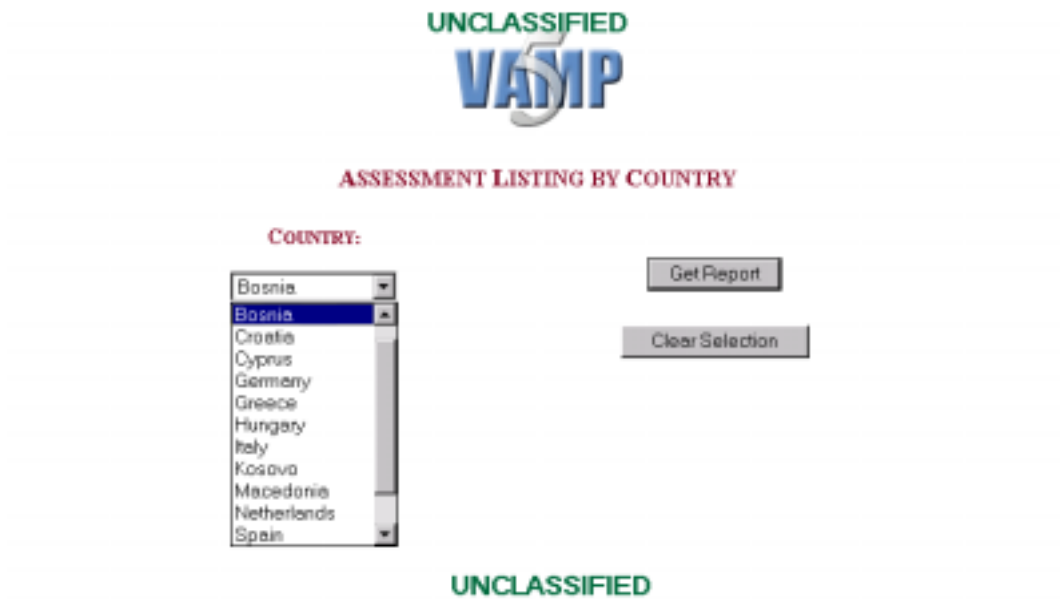


Figure M-1-A-4

**M-2-A-4**

**FOR OFFICIAL USE ONLY**



**FOR OFFICIAL USE ONLY**

**(3) City.** Access assessment data by city. Useful report to retrieve data for cities with more than one installation/activity.

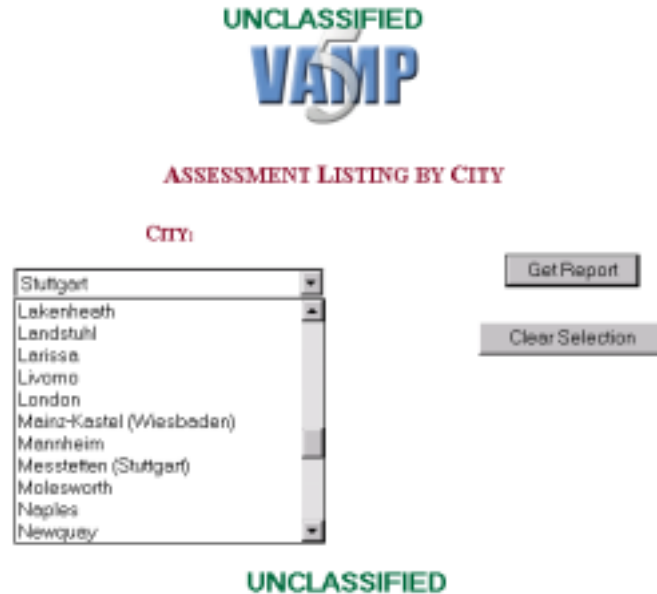


Figure M-1-A-5

**(4) Threat Level.** Access assessment data by Threat Level at the time of the assessment, not the current Threat Level. Useful report for historical data showing installation vulnerabilities identified during a particular Threat Level for comparison to posture in current Threat Level. Since it is historical data, old Threat Levels (Medium and Negligible) are available options. Valuable report to review subsequent to an increase in Threat Level.



Figure M-1-A-6

**(5) FPCON.** Access assessment data by FPCON at the time of the assessment, not the current FPCON. Useful report for historical data showing

**M-2-A-5**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

installation vulnerabilities identified during a particular FPCON for comparison to posture in current FPCON. Valuable report to review following, or while considering, an FPCON change.



Figure M-1-A-7

**(6) Program Assessment.** Access assessment data by unit commander's Program Assessment of the AT Program based on the installation's ability to meet the eight critical AT Program requirements established in this OPOD (see Annex M, Appendix 2, para 7). Provides commanders with the ability to quickly identify the status of programs for which they have FP responsibility.



Figure M-1-A-8

**(7) Assessment Team.** Access assessment data by team that conducted the assessment. Provides users the ability to research findings of specific teams.



Figure M-1-A-9

**FOR OFFICIAL USE ONLY**

**(8) Force Protection Status.** Provides table displaying the status for each installation/activity in the command. Table includes FPCON and Threat Level, Commander's Program Assessment, and information on last assessment.

NOTE: The display below is from the VAMP Training database based on fictional observations and does not reflect actual status of any EUCOM programs.



**Force Protection Status**  
Current as of 19-Aug-01

AT Program Assessment  
RED: 0  
AMBER: 1  
GREEN: 2

Sort Order: AT Program Assessment Color/Installation

Installation - Entity Address City, Country	FPCON Threat Level (Assessment/Status)	Component (Assessment Type)	Commander's AT Program Assessment	Last Assessment Assessment Team	Next Assessment Assessment Team
Example AB - NAME Hannover, Germany	Extreme/Alpha Moderate/Moderate	STAFF (294.30)	AMBER	EL.Aug01 HQ/17A	EL.Nov01 TBD
Example B - NAME Oberammergau (Straubing), Germany	Extreme/Alpha Moderate/Moderate	USAFR19 (294.30)	GREEN	EL.Aug01 Eggle HQ	EL.Aug01 TBD

Figure M-1-A-10

**(9) Archived Data.** Recall archived data by installation. VAMP 5.0 allows users to archive (or delete) data no longer needed. VAMP 5.0 does not eliminate archived data, so this report provides a very useful option to review previous decisions or findings. For example, mitigated vulnerabilities can be archived and recalled at a later date if necessary. Once archived, information can be retrieved back to the active database by simple request to ECSM. Recommend archiving completed observations after subsequent HHQ or local vulnerability assessments (VA) and archiving original observations if subsequent VA identifies the observation as a repeat and only maintain the repeat observation in the active data. Do not archive current vulnerabilities mitigated through compensatory measures or those the commander has determined to accept following a risk assessment.



Figure M-1-A-11

**FOR OFFICIAL USE ONLY**

**(10) Edit/Update Data.** After retrieving a report based on one of the report criteria--except Archived Data which cannot be edited or updated--user is linked to screens similar to the next two. The first lists all available assessments, and the user should select the desired assessment based on the assessment date. The second screen lists the specific observations during the selected assessment.

NOTE: The following displays are from the VAMP Training database based on fictional observations and do not reflect actual status of any EUCOM programs.

**MULTIPLE INSTALLATION RECORDS FOUND**

Select one from the following:

INSTALLATION:	UNIT/ACTIVITY:	ASSESSMENT DATE:	ASSESSMENT TEAM:	ASSESSMENT STATUS:
Test Base Alpha	ACC	27 Jun 01	DTRA	<span style="background-color: red; color: white; padding: 2px;">RED</span>
Test Base Alpha	AFMC	12 Jun 01	J5VA	<span style="background-color: red; color: white; padding: 2px;">RED</span>

RETURN

Figure M-1-A-12

Installation: Test Base Alpha RED  
VIEW ASSESSMENT

Unit/Activity: AFMC - State 1, United States

<b>SUMMARY:</b>	Excellent AT/FP program; superior relationship between FP NCO and wing staff--extremely effective force protection working group relationship. Need to exercise entire plan
-----------------	---

PROJECT:	CATEGORY:	VULNERABILITY:
<a href="#">AFMC-15-B11000</a>	Infrastructure - Force Protection	No firefighting water supply for dormitory 200.

RETURN

Figure M-1-A-13

**(a)** Select Project Number hyperlink to see recapitulation of the vulnerability. This is a view only option and does not provide an edit capability.

**(b)** Select Vulnerability hyperlink to edit or update data in any of the six data entry points. To change data, select the link on the top of the observation banner (See Figure M-1-A-14). The link goes to another screen to allow data changes (Figure M-1-A-15). Recommend changing data on only one screen at a time and commit the data after each screen change. **IMPORTANT:** Data will not change unless user selects the "Commit" button at the bottom of the page. For brevity, only three data change screens are shown in the OPORD, but all six have similar features. Selecting the "Edit" button links to the original data entry point.



**FOR OFFICIAL USE ONLY**

**(11) Archive/Delete Data.** Use the same retrieval process to Archive/Delete as to Edit/Update. Refer to paragraph 4c(10) and Figures M-1-A-12 and M-1-A-13, above. Instead of selecting the Edit/Update link on the top banner, select the Archive/Delete link on the bottom banner. Archived/Deleted data actually remains on the server but is inaccessible to the installation user so it provides the ability to reduce the size of your active data without losing historical data. In order to retrieve archived data, simple send a request through the component command AT/FP office to the USEUCOM VAMP administrator (ECSM) to restore the data into the active database. Data will normally be restored within a few days of the request.



**d. Generate User-Definable Reports.** Provides several report options.

**(1) Query Observation by Text String.** Very powerful report that allows users to select all observations matching user defined criteria. For example, user can select all observations specifying *barriers* or any other criteria in the Observation, Discussion, or Options blocks. User also can recall all observations under a specific category (i.e., Perimeter/Access Control). Report can be limited to specific installation or include all occurrences throughout the command. Very useful report to identify specific issues impacting plans/procedures or determining programmatic issues for developing budget submissions.



Figure M-1-A-16

**M-2-A-10**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**(2) Dynamic Query.** VAMP-determined, user-selected criteria to prioritize observations. Limited applications.

**(3) Rank by Score (Original).** Original report prioritizes all vulnerabilities within a specific command. Report options include number of vulnerabilities (10, 20, 50, 100, or All); shows completed vulnerabilities or not; and specific component. Useful for component AT/FP offices to identify most significant vulnerabilities in the command.

**(4) Rank by Score (Installation).** Similar to original report except limited to a particular installation. Report options include number of vulnerabilities (10, 20, 50, 100, or All) and show completed vulnerabilities or not. Useful for installation ATO to identify most significant issues and also to identify potential programming (POM, BAM, or CbT RIF) issues.



**FOR OFFICIAL USE ONLY**

**(5) Custom Report.** Best for installation users requesting report based on specific fields shown below. User checks boxes to identify desired information. VAMP e-mails data in spreadsheet format which user can modify with MS Excel program.

VAMP (MAIN) INFO		OBSERVATIONS INFO		CORRECTIVE ACTION INFO	
Available Report Columns	Show Columns	Available Report Columns	Show Columns	Available Report Columns	Show Columns
Installation	<input type="checkbox"/>	Observation Number	<input type="checkbox"/>	Design Status	<input type="checkbox"/>
City	<input type="checkbox"/>	Tracking Number	<input type="checkbox"/>	Project Status	<input type="checkbox"/>
Country	<input type="checkbox"/>	Send To Higher	<input type="checkbox"/>	Design Status Percent Complete	<input type="checkbox"/>
Unit/Activity	<input type="checkbox"/>	Assessment Category	<input type="checkbox"/>	Project Status Percent Complete	<input type="checkbox"/>
Parent Command	<input type="checkbox"/>	Observation	<input type="checkbox"/>	Estimated Start Date	<input type="checkbox"/>
Component HQ Responsible	<input type="checkbox"/>	Discussion	<input type="checkbox"/>	Estimated Completion Date	<input type="checkbox"/>
Assessment Team	<input type="checkbox"/>	Options	<input type="checkbox"/>	POC	<input type="checkbox"/>
Threat Level	<input type="checkbox"/>	(0) Command Priority	<input type="checkbox"/>	Host Nation Approved	<input type="checkbox"/>
FPCOn	<input type="checkbox"/>	(0) Access Controls	<input type="checkbox"/>	Funded	<input type="checkbox"/>
AT Program Assessment	<input type="checkbox"/>	(0) Population Centers	<input type="checkbox"/>	CBTRIF	<input type="checkbox"/>
Last Assessment Date	<input type="checkbox"/>	(0) Symbolic Value	<input type="checkbox"/>	Component Priority	<input type="checkbox"/>
This Assessment Date	<input type="checkbox"/>	(0) Equipment	<input type="checkbox"/>	Unit Priority	<input type="checkbox"/>
Next Assessment Date	<input type="checkbox"/>	(0) Mitigation	<input type="checkbox"/>	Cred Eng. Project No	<input type="checkbox"/>
Summary	<input type="checkbox"/>	(0) AT Progress	<input type="checkbox"/>	Obligation Year	<input type="checkbox"/>
Mission	<input type="checkbox"/>	(0) Seize	<input type="checkbox"/>	National Stock Number	<input type="checkbox"/>
Commander's Summary	<input type="checkbox"/>	Other Facilities Affected	<input type="checkbox"/>	Model Number	<input type="checkbox"/>
Assessment Type	<input type="checkbox"/>			Part Number	<input type="checkbox"/>
Data Record Added	<input type="checkbox"/>			Item Number	<input type="checkbox"/>
				Vendor Name	<input type="checkbox"/>
				Corrective Actions Completed	<input type="checkbox"/>
				Cost (numeric)	<input type="checkbox"/>
				Cost (alpha)	<input type="checkbox"/>

Figure M-1-A-17

**(6) Resources Worksheet.** Provides data for Joint Staff-format spreadsheet to identify unfinanced requirements. Allows user to select data by Installation and e-mail report to requestor. VAMP e-mails data in spreadsheet format which user can copy and paste into Joint Staff spreadsheet. (Tip: Copy entire VAMP-provided report and paste into J34 spreadsheet. Then format the cells to “wrap text”) Data is only available for each programmatic vulnerability if user entered either at the time of initial entry or during monthly reviews. Specific data requirements are addressed in Add Observation instructions within this Appendix.

**e. Available System Reports**

**(1) JSIVA Reports.** Allows user to request out-briefs and written reports from previous JSIVAs for units within the same component command. VAMP e-mails briefing (MS PowerPoint) or written report (Adobe and/or MS Word) to user.



**FOR OFFICIAL USE ONLY**

**(2) Installation Status Report.** Provides consolidated on-screen report for installation senior leadership to review the installation top 10 vulnerabilities. Report displays only programmatic vulnerabilities as the default, although user has the option to include procedural vulnerabilities. Report displays project number, description of the observation (vulnerability), current status, and installation point of contact.

NOTE: The display below is from the VAMP Training database based on fictional observations and does not reflect actual status of any EUCOM programs.



Figure M-1-A-18

**(3) Charts and Metrics.** Reports primarily used by VAMP administrators; so, specific data for each report is excluded from the OPORD.

**(4) AOR Threat Level/FPCON.** Provides report on AOR Threat Levels and FPCONs. Report available in table format by Threat Level and FPCON, or in an alphabetical list by country showing Threat Level, installation FPCON levels, and date of last change. Useful historical report for pre-deployment planners.

**(5) VAMP Revision History.** Compilation of changes to VAMP since original release on 21 Jan 98.

**f. Messages.** This section provides easy access to messages with significance to the VAMP such as the yearly Joint Staff JSIVA Trends message.

**FOR OFFICIAL USE ONLY**

**g. Enter Assessment/Update Threat Status.** The starting point for entering observations into the VAMP and, as such, the most important section of the VAMP. The drop down menu provides two choices: Add Observation and Update AOR Threat Levels/FPCONS.

**(1) Add Observation.** There are six screens in the process to add an observation into the VAMP:

**(a) Unit/Activity Screen.** First, the user selects the echelon of command with responsibility for force protection (Army - ASG/BSB; Air Force - Wing; and Navy - Installation).



Figure M-1-A-19

**(b) Installation Screen.** Next, the user selects specific community, base or site then inputs data relative to the assessment. Assessment specific data includes the Team Summary (copy and paste from written report) and Commander's Summary.



Figure M-1-A-20

**M-2-A-14**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

-- Eight Critical Program Requirements are derived from DODI 2000.16 and identified in this OPOD. Selecting "No" on any one of these requirements results in a program assessed as Red.

-- Commander's Summary is critical since this is the first place to identify commander's assessment of his/her AT/FP program; priorities of work to address each vulnerability; and document any risk assessment decisions. The commander can also use this area to document decisions to change the overall program assessment for Green to Amber or Red. Although it should be noted a commander cannot change a program assessment from Red to Amber or Green without correcting the deficiency if it is one of the eight Critical Program Requirements.

*Critical Program Requirements*

- Yes  No 1. Comprehensive AT Program Established (Standard 2)
- Yes  No 2. Trained Force Protection Officer Assigned in Writing (Standard 6)
- Yes  No 3. Local Threat Assessment Conducted Within Last 12 Months (Standard 15)
- Yes  No 4. Written, Executable AT Plan Fully Coordinated with Tasked Units (Standard 14)
- Yes  No 5. AT Plan Exercised Annually and Lessons Learned Written (Standard 19)
- Yes  No 6. Comprehensive Local Vulnerability Assessment Conducted Annually (Standard 26)
- Yes  No 7. Threat Information Notification System Established (Standard 9)
- Yes  No 8. Countermeasures In-Place to Mitigate Known Vulnerabilities (Standard 14)

---

**Enter Assessment Team Summary:**

Not Specified

Suggested length: 255 characters  
This assessment's 'Risk' must not be classified higher than 'Secret (S)'

**Enter the Commander's Summary:**

Not Specified

Figure M-1-A-21

**(c) Observation Screen.** User inputs Observation, Discussion, Options. First, select the specific category from the drop down list. Categories are limited to major areas in the JSIVA reports and the same categories should be used for local assessments.

**OBSERVATION INFORMATION**

**Category:** Infrastructure - Fire Protection

- Infrastructure - Fire Protection
- Infrastructure - Utilities - Comm
- Infrastructure - Utilities - Electric
- Infrastructure - Utilities - Fuels
- Infrastructure - Utilities - Water
- Infrastructure - Weapons of Mass Destruction
- Operations Readiness - Contingency Planning
- Operations Readiness - Emergency Response
- Operations Readiness - Training and Exercises
- Operations Readiness - Weapons of Mass Destruction
- Security Operations - Executive and Personal Protection

**Observation:**

Input. The data contained in these fields (the information in green (original data) is) can't be changed.

Figure M-1-A-22

**FOR OFFICIAL USE ONLY**

-- Enter *Observation* data by either “copy and pasting” from the written report or compose the observation data directly into VAMP. Funding decisions and command risk assessments may be based on the information in this block, so the data should be specific so as to be easily understood by anyone reading it. Length of the input is only limited by other program restrictions (i.e., any data printed to an Excel spreadsheet is limited to 255 characters per field). While the VAMP observation block will accept pages of data, observation should be concise and specific.

-- User must also annotate the appropriate classification otherwise VAMP will return an error message. Use the JSIVA observation classification or for local assessments refer to Annex L of this OPORD for guidance.

**Help**  
The following three text input fields have been emptied to facilitate input. The data contained in these fields is still in the database. If you copy new information into the following three fields, the information in green (original data) will be replaced. Otherwise, the Observation, Discussion, and Options fields will remain unchanged.

**Observation:**  
Link

Maximum Length: 255 Character  
Data entered will not be classified higher than Secret (S)

**Provide a Classification for this Observation:**

**Classification:**  (U) If classified (C) or (S), can this text be RELEASED?  
 (F) If Yes, key is RELEASE - is , NATO, BSM, FBI, or  
 (S) IF NOT RELEASEABLE, how this input Mark

[Classification Help](#)  (C) If classified (C) or (S), is this classification:  Original  Derived

If classified (C) or (S), provide declassification date:

Or specify declassification event:

Or provide Ten-Year Duration date:

Or click exceptions to the ten-year rule:

Figure M-1-A-19

The *Discussion* and *Options* blocks are on the same page as the *Observations*, user should “copy & paste” from original report or directly input options.

**Discussion:**

Maximum Length: 255 Character  
Data entered will not be classified higher than Secret (S)

**Options:**  
Link

Maximum Length: 255 Character  
Data entered will not be classified higher than Secret (S)

**Observation POC:**  
Link

Maximum Length: 255 Character

**Presubmit Observations:**  Yes  No

**This rating / marking?**  Yes  No

**Other Facilities Allowed?**  DODS  DGA  SOCCER  INTRANS.COM  
 USSPACECOM  NCETR  MARFORDIR

**Do Plans Exist?**  Yes  No

Figure M-1-A-23

**M-2-A-16**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

-- Use the *Discussion* block to input discussion directly from the JSIVA report or to further clarify an observation. This is the area to amplify the observation with details to clearly describe the vulnerability for others not familiar with the observation. Also, this is an area to identify a commanders risk assessment decision following an assessment, either HHQ or local.

NOTE: If documenting a commander's risk assessment decision use the abbreviation "CRA" at the end of the text in the *Discussion* block. Specifically, adding "CRA" will allow users to search the database and identify all observations and/or vulnerabilities for which the commander has accepted the risk. This is the area to document commander's decision to mitigate impact of vulnerabilities that are either impractical or too costly to correct. For example, if a dormitory is within 10 meters of a perimeter wall bordering an off-base road and the commander has decided to accept the risk in lower FPCONs, document the decision in the *Discussion* block. Also, include the appropriate compensatory measures in place to reduce the risk in higher FPCONs. This will be especially useful to brief new commanders on existing vulnerabilities accepted by the previous commander and the installations compensatory measures to mitigate the risk.

-- Use the *Options* block to identify specific alternatives including tactics, techniques and procedures to mitigate the vulnerability. Do not necessarily address only resource requirements or technologies. Ensure the *Observation POC* is accurate and not always the AT Officer/NCO. For example, an observation in the Fire Dept should probably identify the Fire Chief as the POC.

-- The default for *Procedural Observation* is "No," so if the observation is procedural select "Yes" and VAMP will not consider this observation in the prioritization of vulnerabilities. The default for *Use Rating / Scoring?* is "Yes" so if this is a procedural observation and the user does not change this setting, the observation will be scored and prioritized with all other vulnerabilities. To eliminate procedural observations from the scoring methodology select "No." Accept the default for programmatic vulnerabilities (those requiring funds) to score and prioritize the vulnerability.

-- Since VAMP only allows users to access vulnerabilities within their Service, users must select the appropriate block if *Other Facilities Affected?* Selecting a block here allows the responsible Agency/Component Force Protection office access to the data. If photos are available and provide a better understanding of the vulnerability, VAMP provides the ability. Again, consider the impact of the photo to better represent your requirements for funding or concerns for risk assessments.

**FOR OFFICIAL USE ONLY**

-- Finally, one of the most important aspects of VAMP is the prioritization methodology. User selects the most appropriate description from each drop down menu. VAMP assigns point values for each area, and the current Threat Level and FPCON, according to the Vulnerability Prioritization Methodology reflected in the following categories.

**RATING AND SCORING**

**Command Priority:**

**Current Breakout of Command Priority**

0 - CRITICAL (Top 10% of Command Priority List--#1 of 10)
0 - HIGH (Top 30% of Priority List--#s 2 & 3 of 10)
0 - MEDIUM (Top 70% of Priority List--#s 4-1 of 10)
0 - LOW (Bottom 30% of Priority List--#s 9 & 10 of 10)

**Installation Access Controls:**

**Population Centers:**

**Symbolic Value:**

**Security Equipment/Construction:**

**Vulnerability Mitigated/Corrective Action Taken:**

**AT Program Effectiveness:**

Figure M-1-A-24

**Command Priority:** Indicates the responsible commander's priority; i.e. Installation, Wing, or ASG/BSB Commander. Commanders can only prioritize their top 10 vulnerabilities in the VAMP methodology. The Current Breakout of Command Priority provides the user with the current numbers of ALL ranked observations for an installation/activity. Do not exceed the limit (one Critical, two High, etc.) otherwise user risks skewing the data.

**Installation Access Controls:** Identify the method of controlling access to the installation/activity, regardless of the location of the vulnerability. For example, a vulnerability resulting from a public roadway adjacent to a fenced installation with U.S. Forces on the entry gates should be identified as U.S. Controlled/Fenced Activity.

**Population Centers:** Refers to the specific vulnerability not the entire installation.

**Symbolic Value:** Self-explanatory

**Security Equipment/Construction:** Select the most appropriate category for the recommended corrective action.

**Vulnerability Mitigated/Corrective Action Taken:** Select the most appropriate rating. If "No Interim Corrective Actions or Compensatory Measures" is the appropriate response, be sure to explain Commander's Risk Assessment decision on the Corrective Actions page.

**AT Program Effectiveness:** Identify the part of the Installation AT Program most significantly impacted by the vulnerability.

M-2-A-18

**FOR OFFICIAL USE ONLY**



**FOR OFFICIAL USE ONLY**

**(d) Corrective Action Screen.** User identifies what, if any, corrective action the installation will take to address the vulnerability.

The screenshot shows a web-based form titled "CORRECTIVE ACTION INFORMATION". At the top, there are navigation tabs: "VULNERABILITY", "INSTALLATION", "DESCRIPTION", "CORRECTIVE ACTION", "FUNDING", and "SUPPLIER". The form fields are as follows:

- Component Priority:** A dropdown menu with "0" selected.
- Unit Priority:** A dropdown menu with "0" selected.
- CE Tracking Number:** A text input field containing "Unk".
- Project Number:** A text input field containing "Unk".
- Start Date:** A date input field containing "24 Apr 01".
- Completion Date:** A date input field containing "24 Apr 01".
- Design Status % Complete:** A text input field containing "0".
- Project Status % Complete:** A text input field containing "0".
- Proj POC at Unit:** A text input field containing "Unk".
- Meets OSTRIF Criteria:** A dropdown menu with "No" selected.
- Are Corrective Actions Completed?:** Two radio buttons, "NO" (selected) and "YES".
- Corrective Action Status:** A large text input field containing "Unk".

Figure M-1-A-25

Component and Unit Priority: No impact; options will be removed under next revision.

CE Tracking Number: CE is Air Force term for Civil Engineer. Input the engineer (Public Works) work order number. Provides ability for long-term project tracking.

Project Number: Enter the funding project number. Normally assigned by the Component Command after the fact. Important to keep this number linked to the CE Tracking Number since projects are funded by Project Number but completed by engineers work order number.

Start Date, Completion Date, Design & Project Status are input once the work actually begins.

Proj POC at Unit: List the person actually responsible, not necessarily the AT NCO or Security Officer.

Corrective Action Status: Limited to 255 characters to fit into an Excel spreadsheet, otherwise characters are unlimited. Use to update the status of steps taken to mitigate the vulnerability; place the date at the beginning of each entry to show when the update was accomplished. Be as specific as possible identifying corrective actions, and if no compensatory measures are possible, identify commander's decision to accept the associated risk.

**(e) Funding Screen.** User completes funding data to identify requirements to higher headquarters. Specific directions for each data entry point are available through the hyperlink "Resource Requirements Worksheet" on the page. Every item must be completed, if unsure input N/A or unknown. For boxes requiring key stroke entries, data is limited to 255 characters since the end product is an Excel spreadsheet. Items to consider:

Obligation Year: Realistically, the obligation year will be the first year of the next PPBS cycle, normally 2 fiscal years from the date entered. For example, data entered in 2002 will normally be considered for funding in FY05 (Oct 04). For

**M-2-A-19**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

emergent or emergency projects, consider funding through the Combating Terrorism Readiness Initiatives Fund (CbT RIF), but still include data in the PPBS cycle since CbT RIF is not a guaranteed source of funding.

INDUSTRY    RETAILER    DISTRIBUTOR    DIRECTOR/ACTOR    FINING    **PPBS/DOE**

---

**FUNDING INFORMATION**

Corrective Action Cost:       Funded:  Yes - No - N/A  
See What's New, i.e., 2000 EIDP, etc. 7

Obligation Year:       Host Nation Approved:  Year from: yyyy, i.e., 2001

---

**Resource Requirements Worksheet**

(a)  Control Number

(b)  Army (A)    Air Force (AF)    Navy (N)    Marine (M) Service / Agency

(c)  Component

(d)  Location / FPCen

(e)  Must (M)    Need (N)    Should (S) Priority

(f)  Requirement Title

(g)  Requirement Description

(h)  Type IFA / Disposition    / MMYFY

---

**JUSTIFICATION**

(i)  High (H)    Significant (S)    Medium (M)    Low (L) Threat  
Description:

(j)  High (H)    Medium (M)    Low (L) Vulnerability  
Description:

(k)  High (H)    Medium (M)    Low (L) Asset Criticality  
Description:

(l)  High (H)    Medium (M)    Low (L) AT Plan Effectiveness  
Description:

---

(m)  High (H)    Medium (M)    Low (L) Commander Risk Assessment  
Description:

(n)  TAB O Category

(o)  PSE Category (if applicable)   (if applicable)

(p)  IPL

(q)  Appropriation

---

**FUNDING REQUIREMENTS (\$M):**

(r)  FY04

(s)  FY05

(t)  FY06

(u)  FY07

(v)  FY08

(w)  FY09

(x)  Yes    No   If Yes, Enter the Year (YYYY):  CbT RIF

Figure M-1-A-26

**M-2-A-20**

**FOR OFFICIAL USE ONLY**



**FOR OFFICIAL USE ONLY**

Funding Requirements (\$M): Ensure you input costs in millions, not thousands. Also consider life-cycle costs for maintenance, repair, or replacement. For example, new radios procured in FY04 will require annual maintenance contracts at the end of the normal 12-month warranty period, so include maintenance costs in FY 06-90. Also, consider the replacement costs for new radios, batteries, etc. after 3-5 years

**(e) Supplier Information Screen.** This section provides continuity and follow-up status for corrective actions requiring resources. Continuity of funding projects and corrective actions is dependent on documenting sources of supply, so it is very important to complete this data entry once user identifies a source of supply.

The screenshot displays the 'SUPPLIER INFORMATION' screen. At the top, a navigation bar includes tabs for 'HIST/ACTIVITY', 'INSTALLATION', 'OBSERVATION', 'CORRECTIVE ACTION', 'FUNDING', and 'SUPPLIER'. The main content area is titled 'SUPPLIER INFORMATION' and contains the following fields:

- Vendor Name:** Unk (with a note: \* If Unknown, enter UNSK)
- Model Number:** Unk (with a note: \* If Unknown, enter UNSK)
- Part Number:** Unk (with a note: \* If Unknown, enter UNSK)
- Item No:** Unk (with a note: \* If Unknown, enter UNSK)
- National Stock No:** Unk (with a note: \* If Unknown, enter UNSK)

At the bottom of the screen, there is a button labeled 'Review Observation'.

Figure M-1-A-27

The next step in adding a new observation is reviewing the data by clicking the "Review Observation" button. The next screen provides a single page view of each piece of data entered on the six screens. Individual pages can be edited by selecting the corresponding "Edit" button, which will return you to the appropriate screen. After correcting the data, continue through the following pages until you return to the Edit Page. It is NOT necessary to re-enter correct data, but you **MUST** select the **COMMIT** button at the bottom of the Edit Page to commit data to VAMP. After committing data, VAMP provides the option to enter new observations same installation; new observation different installation; or exit VAMP.

**FOR OFFICIAL USE ONLY**

**(2) Update AOR ThreatLevels/FPCONs.** Allows user to update FPCONs at each installation. Users must update FPCONs as soon as practical after a change. ECSM will update the Threat Levels. To update FPCONs, select the box next to the specific country then select the “Expand” button at the bottom of the page. All installations listed in the VAMP for the specific country will be displayed on the next screen. Simply change the FPCON and select “Submit” button at bottom of page. Next screen will show changes and allow user to either “Cancel” or “Verify.” “Verify” enters change and VAMP automatically notifies all component command AT/FP offices and ECSM as part of the nightly update.

**EUCOM AOR THREAT LEVELS / THREAT CONDITIONS**  
VAMP

**PLEASE NOTE:**  
THREATLEVELS are designated at the COUNTRY level (only). THREATCOND are designated at the COUNTRY and INSTALLATION (optional) levels. The list is sorted alphabetically by [Country, City - Installation].

To EXPAND or CONTRACT data for a country, check the appropriate box and click the corresponding button. Setting THREATLEVELS / THREATCOND requires that a selection be made from the associated drop-down and clicking the SUBMIT button.


Current Observation Scores are recalculated on the hour. When changes to THREATLEVELS / THREATCOND are submitted, the scores will be updated at the next recalculation.

---

<input type="checkbox"/> <b>United Kingdom</b>	<b>Moderate</b> ▾	<b>Normal</b> ▾	
Alconbury - RAF Alconbury		<b>Alpha</b> ▾	
Barford St. Johns - RAF Mildenhall (Barford St. Johns)		<b>Charlie</b> ▾	
Chicksands - RAF Mildenhall (Chicksands)		<b>Bravo</b> ▾	
Croughton - RAF Croughton		<b>Delta</b> ▾	
Digby - RAF Mildenhall (Digby)		<b>Normal</b> ▾	

---

<input type="checkbox"/> <b>Ukraine</b>	<b>Low</b> ▾	<b>Charlie</b> ▾	
<input type="checkbox"/> <b>United Kingdom</b>	<b>Moderate</b> ▾	<b>Charlie</b> ▾	
<input type="checkbox"/> <b>Zambia</b>	<b>Low</b> ▾	<b>Charlie</b> ▾	
<input type="checkbox"/> <b>Zimbabwe</b>	<b>Low</b> ▾	<b>Charlie</b> ▾	



**PLEASE NOTE:**  
THREATLEVELS are designated at the COUNTRY level (only). THREATCOND are designated at the COUNTRY and INSTALLATION (optional) levels. The list is sorted alphabetically by [Country, City - Installation].

To EXPAND or CONTRACT data for a country, check the appropriate box and click the corresponding button. Setting THREATLEVELS / THREATCOND requires that a selection be made from the associated drop-down and clicking the SUBMIT button.

Current Observation Scores are recalculated on the hour. When changes to THREATLEVELS / THREATCOND are submitted, the scores will be updated at the next recalculation.

For additional information, please contact [vampSupport](#).

VAMP is a product of the Headquarters United States European Command, Office of the Special Assistant for Security Matters (ECSM).

Figure M-1-A-28

**FOR OFFICIAL USE ONLY**

**h. User Account Utilities.** Allows users to make limited changes to their accounts. Important for first-time users to verify accuracy of their contact information, especially e-mail address, and to change their assigned password.

**(1) Update Contact Information.** Users should modify this data as often as necessary to maintain accuracy. Two key pieces of data are the e-mail address and DSN phone number. Simply replace old data and update.

**UPDATE CONTACT INFORMATION**

Fill in all blanks and update information as necessary. All items are required.

VAMP Login ID: LyachD

Rank:	<input type="text"/>	Input your rank. If civilian, enter Civ
First Name:	<input type="text"/>	Input your first name.
Last Name:	<input type="text"/>	Input your last name.
Command:	<input type="text"/>	Enter your duty command.
Directorate:	<input type="text"/>	Enter your directorate.
Email Address:	<input type="text"/>	Enter your SIPRNet email address.
DSN Phone:	<input type="text"/>	DSN phone number.
Civilian Phone:	<input type="text"/>	Enter your commercial phone number.

---

Figure M-1-A-24

**(2) Change Password.** Self-explanatory. Recommend changing assigned password during first entry into VAMP. Notify the USEUCOM VAMP administrator in the event you forget your username or password. The administrator will send username and password to the e-mail address on record in the VAMP.

#### **4. Reporting Problems or Recommending Changes**

**a.** Report any problems to the component VAMP administrator. If the component administrator is unable to correct the problem, then he/she will forward the issue to the USEUCOM administrator (ECSM).

**b.** VAMP is an evolving program currently under the 5th revision and ECSM continually solicits inputs from users to improve the program effectiveness. Provide any suggested changes to the component administrator for review and/or recommendation.

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**M-2-A-24**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### **TAB B (COMPONENT COMMAND ASSESSMENT CHECKLIST) APPENDIX 2 (VULNERABILITY ASSESSMENTS) TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPOD 01-01**

#### **REFERENCES: See Basic Order**

This OPOD, DoD Directive 2000.12, and DoD Instruction 2000.16 require the CINC to review the AT/FP Program and Plan of the Service component commands at least annually. The following checklist is a guide for conducting HQ USEUCOM AT/FP program reviews. The review will focus on the Service component commands' plans and policies which are designed to ensure their subordinate commands are in compliance with applicable directives.

The HQ USEUCOM team, led by the Special Assistant for Security Matters (ECSM), will include personnel from ECSM, ECJ23, and ECJ4-ENG. In addition to using the following checklist as a guide for determining compliance with DoD and HQ USEUCOM AT/FP directives, the team will review issues and initiatives impacting on the commands' capabilities and overall program effectiveness. Additionally, team member(s) will accompany the Service component command's Vulnerability Assessment team on one Standard 26 assessment, as defined in Annex M, Appendix 1.

## FOR OFFICIAL USE ONLY

ITEM	COMPONENT COMMAND ASSESSMENT CHECKLIST ITEMS	Rating Go/No Go R/A/G	REMARKS (All references are keyed to this OPORD unless otherwise indicated.)
<b>Component Commander Specific Responsibilities for AT/FP Program:</b>			
<b>1</b>	Designate and report to HQ USEUCOM the AT/FP program POC(s) <b>(Basic Order, para 3d(2)(c))</b>		
<b>2</b>	Notify ECSM of any conflicting, policies, procedures, and/or directives <b>(Basic Order, para 3d(2)(d))</b>		
<b>3</b>	Develop internal AT/FP plans and policies, and incorporate all OPORD 01-01 requirements into plans <b>(Basic Order, para 3d(2)(e))</b>		
<b>4</b>	Ensure each deployed/stand alone unit has an assigned/trained AT Officer (ATO) <b>(Basic Order, para 3d(2)(f))</b>		
<b>4a</b>	Individual aware of methods available for obtaining AOR-specific updates for deployment/travel area <b>(Annex M, Appendix 1, para 4f (Standard 6))</b>		
<b>4b</b>	Individual understand materials for Level I instruction and able to support Commander's AT program <b>(Annex M, Appendix 1, para 4f (Standard 6))</b>		
<b>5</b>	Manage Terrorist Treat information through the following actions: <b>(Basic Order, para 3d(2)(g))</b>		
<b>5a</b>	Gather, analyze, disseminate terrorist threat information		
<b>5b</b>	Ensure subordinate and support units report information on potential threats		
<b>6</b>	Ensure subordinate and support units report information on potential threats <b>(Basic Order, para 3d(2)(g))</b>		
<b>6a</b>	Ensure proper dissemination and implementation of Force Protection Condition procedures & measures		
<b>6b</b>	Ensure changes are transmitted rapidly to all DOD elements in the affected area and through the chain of command		
<b>7</b>	Provide required resources for AT/FP through Service (USSOCOM for SOCEUR) funding channels <b>(Basic Order, para 3d(2)(i))</b>		
<b>8</b>	Provide HQ USEUCOM/ECSM a quarterly listing of all unfunded AT/FP rqmts meeting CbTRIF criteria <b>(Basic Order, para 3d(2)(j))</b>		
<b>8a</b>	List includes a priority rank ordering of the items and results of Service funding process		

**FOR OFFICIAL USE ONLY**

<b>ITEM</b>	<b>COMPONENT COMMAND ASSESSMENT CHECKLIST ITEMS</b>	<b>Rating Go/No Go R/A/G</b>	<b>REMARKS (All references are keyed to this OPORD unless otherwise indicated.)</b>
<b>8b</b>	Use the Vulnerability Assessment Management Program (VAMP) to assemble data and prioritize input		
<b>9</b>	Conduct a HHQ VA of all subordinate commands and activities periodically <b>(Basic Order, para 3d(2)(l-n))</b>		
<b>9a</b>	Base frequency on the current Terrorism Threat Level but no less than once every 3 years		
<b>9b</b>	Ensure this assessment meets all the requirements as stated in USEUCOM AT/FP Prescriptive Program Standard 6		
<b>9c</b>	Ensure assessment team has the requisite expertise for the required areas		
<b>9d</b>	Coordinate with ECSM the execution of any Service, JSIVA, or other HHQ VA		
<b>9e</b>	Send a representative to accompany JSIVA teams		
<b>9f</b>	Notify ECSM when scheduling and executing any off-cycle assessments		
<b>10</b>	VAMP Management <b>(Basic Order, para 3d(2)(n-p), &amp; Annex M, Appendix 2, Tab B)</b>		
<b>10a</b>	Report assessment results to ESCM using the online VAMP on the SIPRNET		
<b>10b</b>	Monitor the VAMP to ensure accuracy of information		
<b>10c</b>	Update the VAMP when changes occur		
<b>11</b>	Ensure all personnel receive AT/FP pre-deployment planning and training prior to deploying into the AOR <b>(Basic Order, para 3d(2)(r))</b>		
<b>12</b>	Identify and coordinate AT resident training to incumbents of high-risk billets and spouses <b>(Annex M, Appendix 1, para 4e (Standard 5))</b>		
<b>13</b>	Ensure tenant units coordinate their AT/FP programs and requirements with the installation commander <b>(Annex M, Appendix 1, para 4p (Standard 16))</b>		
<b>14</b>	Participate in the USEUCOM JAWG and GOASG <b>(Basic Order, para 3d(2)(s))</b>		
<b>15</b>	Develop a process to track documented vulnerabilities <b>(Basic Order, para 3d(2)(o)-(q))</b>		
<b>15a</b>	Review and effectively mitigate all documented vulnerabilities		

**FOR OFFICIAL USE ONLY**

<b>ITEM</b>	<b>COMPONENT COMMAND ASSESSMENT CHECKLIST ITEMS</b>	<b>Rating Go/No Go R/A/G</b>	<b>REMARKS (All references are keyed to this OPORD unless otherwise indicated.)</b>
<b>15b</b>	Validate all vulnerabilities & shortfalls cannot be adequately addressed using existing resources		
<b>Component AT/FP Plan Must:</b>			
<b>16</b>	Fully implement a comprehensive AT/FP program (Annex M, Appendix 1, para 4e (Standard 5))		
<b>16a</b>	Address areas outlined in DoDI 2000.16 and, as a minimum, the specific USEUCOM requirements (Annex M, Appendix 1, para 4b & n (Standard 2 & 14))		
<b>16b</b>	Use intelligence analyses to develop/update plans and programs to protect assets (Annex M, Appendix 1, para 4g (Standard 7))		
<b>17</b>	Deny clearances to Moderate, or higher, Terrorism Threat Level areas until pre-deployment training is verified (Annex M, Appendix 5, para 3b(3))		
<b>18</b>	Address coordinated AT/FP efforts (to include Intel and CI) with host nation authorities and the COM (Annex M, Appendix 1, para 4d (Standard 4))		
<b>19</b>	Ensure HHQ comprehensive VAs of subordinate activities, including off-installation housing (Annex M, Appendix 1, para 4z (Standard 26))		
<b>20</b>	Familiarize personnel with the DoD Terrorism Threat Level classification system (Annex M, Appendix 1, para 4g (Standard 7))		
<b>20a</b>	Task organizations to collect, analyze, and disseminate terrorist threat information (Annex M, Appendix 1, para 4h (Standard 8))		
<b>20b</b>	Address procedures for personnel to report information on events that could threaten DoD personnel/resources (Annex M, Appendix 1, para 4h (Standard 8))		
<b>21</b>	Address Commanders conduct terrorist threat assessment process for their AOR (Annex M, Appendix 1, para 4g (Standard 7))		
<b>21a</b>	Include assessments in the risk assessment development process and appropriate plans (Annex M, Appendix 1, para 4g (Standards 7))		
<b>21b</b>	Form basis for FP enhancements; budget requests & setting Force Protection Conditions (Annex M, Appendix 1, para 4g (Standard 7))		



**FOR OFFICIAL USE ONLY**

ITEM	COMPONENT COMMAND ASSESSMENT CHECKLIST ITEMS	Rating Go/No Go R/A/G	REMARKS (All references are keyed to this OPORD unless otherwise indicated.)
22	Maximize dissemination of all terrorist threat information involving DoD personnel or assets in the AOR (Annex M, Appendix 1, para 4i (Standard 9))		
22a	Include ALL personnel for whom the command has FP responsibility IAW existing MOAs		
22b	Address procedures for using BLUE DARTs to provide actionable, time-critical warning to threatened units (Annex B, Appendix 3)		
23	Identify the Force Protection Condition transition process (Annex M, Appendix 1, para k-m (Standards 11-13) & Annex C, Appendix 2, Tab B))		
23a	Include intelligence, law enforcement, command liaisons (Annex C, Appendix 2, Tab B)		
23b	Apply all applicable measures in the Force Protection Condition system (Annex C, Appendix 2, Tab B)		
23c	Ensure any measures not implemented are reported through chain of command (Annex C, Appendix 2, Tab B)		
23d	Prohibit deviations from down-channeled Force Protection Conditions without prior approval (Annex C, Appendix 2, Tab B)		
23e	Provide procedures to ensure all subordinate units comply with Annex C, Appendix 2 (Annex M, Appendix 1, para 4k (Standard 11))		
24	Ensure subordinate commands conduct VAs at each facility, installation and operating agencies (Annex M, App 1, para 4t & z (Standards 20 & 26))		
24a	VA includes <u>every</u> unit residing on an installation, including tenants, and off-installation housing		
24b	VA teams use Component Command tailored checklists and this OPORD as a guide		
24c	Assessments identify vulnerabilities AND solutions		
24d	Develop a security strategy to mitigate the vulnerabilities found at non-controlled or off-installation facilities (Annex C, Appendix 2, Tab C)		

**FOR OFFICIAL USE ONLY**

ITEM	COMPONENT COMMAND ASSESSMENT CHECKLIST ITEMS	Rating Go/No Go R/A/G	REMARKS (All references are keyed to this OPORD unless otherwise indicated.)
24e	Either secure the facility or relocate the activity if cost-effective solution unavailable to mitigate vulnerabilities. (Annex C, Appendix 2, Tab C)		
24f	Frequency of assessments IAW OPORD 01-01, Table M-1-4		
25	Ensure every subordinate commander has a physical security plan as part of AT/FP program (Annex M, Appendix 1, para 4n (Standard 14))		
25a	Subordinate plan must address facilities, equipment and personnel training for all DoD personnel on the installation		
25b	Subordinates review plans annually or when threat levels change		
25c	Component Command aware of any Vilnability countermeasure deficiencies		
26	Ensure subordinates exercise AT/FP plans annually (Annex M, Appendix 1, para 4s (Standard 19))		
27	Include routine reviews of effectiveness of daily physical security measures and process to adjust as needed (Annex M, Appendix 1, para 4p (Standard 16))		
28	Provide guidance for off installation housing selection and assessments (Annex M, Appendix 1, para 4dd (Standard 30))		
29	Enforce compliance with USEUCOM Force Protection Design Standards (Annex D, Appendix 1)		
29a	Ensure <b>all</b> new construction incorporates the mandatory security engineering concepts (Annex D, Appendix 1)		
29b	Ensure inclusion of additional engineering concepts for permanent construction or major renovation projects (Annex D, Appendix 1)		
29c	Direct inclusion of specific engineering concepts for <u>temporary</u> structures, in addition to the minimum (Annex D, Appendix 1)		
29d	Direct inclusion of specific engineering concepts for <u>expeditionary</u> structures, in addition to the minimum (Annex D, Appendix 1)		

**FOR OFFICIAL USE ONLY**

<b>ITEM</b>	<b>COMPONENT COMMAND ASSESSMENT CHECKLIST ITEMS</b>	<b>Rating Go/No Go R/A/G</b>	<b>REMARKS (All references are keyed to this OPORD unless otherwise indicated.)</b>
<b>30</b>	Ensure installation commanders <u>certify</u> FP considerations are incorporated into the design process <b>(Annex D, Appendix 1)</b>		
<b>31</b>	Identify the process, funding, etc. to train installation engineers and security managers in "Security Engineering" <b>(Annex D, Appendix 1)</b>		
<b>32</b>	Identify the process to request deviations to design criteria <b>(Annex D, Appendix 1)</b>		
<b>33</b>	Ensure commanders develop a prioritized list of factors for site selection teams to determine facility protection level <b>(Annex M, Appendix 1, para 4cc (Standard 29))</b>		
<b>34</b>	Identify procedures for deploying units conduct of pre-deployment VAs and required training <b>(Annex M, Appendix 1, para 4aa (Standard 27))</b>		
<b>35</b>	Ensure each installation, activity or deploying unit appoints a trained (Level II) ATO <b>(Annex M, Appendix 1, para 4x (Standard 24))</b>		
<b>36</b>	Provide a process to encourage family members to receive AT Level I training <b>(Annex M, Appendix 1, para 4v (Standard 22))</b>		
<b>37</b>	Identify process to report personnel arriving in the AOR without required AT training and report deficiency to Service and ECSM <b>(Annex M, Appendix 1, para 4w (Standard 23))</b>		
<b>38</b>	Provide process to annually brief DoD personnel and families on appropriate conduct in a hostage situation <b>(Annex M, Appendix 1, para 4w (Standard 23))</b>		
<b>39</b>	Ensure each installation prepares an incident response plan and conducts frequent drills to familiarize personnel with the plan <b>(Annex M, Appendix 1, para 4q (Standard 17))</b>		
<b>40</b>	Ensure installation incident response plans include security arrangements for all DoD personnel & families living on economy <b>(Annex M, Appendix 1, para 4q (Standard 17))</b>		
<b>41</b>	Identify procedures for supplemental security measures for certain high-ranking DoD officers <b>(Annex M, Appendix 1, para 4ee (Standard 31))</b>		

**FOR OFFICIAL USE ONLY**

<b>ITEM</b>	<b>COMPONENT COMMAND ASSESSMENT CHECKLIST ITEMS</b>	<b>Rating Go/No Go R/A/G</b>	<b>REMARKS (All references are keyed to this OPORD unless otherwise indicated.)</b>
<b>41a</b>	Ensure individuals aware of their responsibilities when accepting supplemental security		
<b>41b</b>	Ensure individuals are cleared for assignment requiring supplemental security and thoroughly briefed on duties of security personnel		
<b>41c</b>	Direct a review of supplemental security needs within 30 days of threat level change		
<b>42</b>	Identify process to develop estimates for potential terrorist use of Weapons of Mass Destruction (WMD) in the AOR <b>(Annex M, Appendix 1, para 4j (Standard 10))</b>		
<b>43</b>	Identify process to assess the vulnerability to terrorist use of WMD affecting their installations/activities <b>(Annex M, Appendix 1, para 4j (Standard 10))</b>		
<b>44</b>	Identify procedures to mitigate the effect of WMD <b>(Annex M, Appendix 1, para 4j (Standard 10))</b>		
<b>Component CI Elements Will:</b> (Appendix 2 to Annex B)			
<b>45</b>	Develop procedures to support commander's incident response plans		
<b>46</b>	Coordinate CI activities that support AT/FP plans and programs through established DoD procedures		
<b>47</b>	Participate in installation VAs as appropriate and within capabilities		
<b>48</b>	Support commanders as they annually exercise AT/FP plans or when threat level or Force Protection Condition change		

**FOR OFFICIAL USE ONLY**

---

(CLASSIFICATION)

**TAB C (VULNERABILITY ASSESSMENT CHECKLIST) TO APPENDIX 2  
(VULNERABILITY ASSESSMENTS AND PROGRAM REVIEWS) TO ANNEX M  
(PHYSICAL SECURITY) TO USCINCEUR AT/FP OPORD 01-01**

**REFERENCES: See Basic Order**

1. This checklist is provided as a stand-alone guide for use by higher headquarters (HHQ) and local Vulnerability Assessment teams when evaluating the Antiterrorism/Force Protection (AT/FP) readiness of installations, sites and facilities in the USEUCOM AOR. USEUCOM Vulnerability Assessment teams use this checklist in conjunction with others when conducting assessments at the installation level.
2. The checklists in Tab D to this Appendix provide additional guidelines and tools to assist in collecting information to support a comprehensive vulnerability assessment. Also, DoD Handbook 2000.12-H and the Defense Threat Reduction Agency (DTRA) Antiterrorism Vulnerability Assessment Team Guidelines provide additional checklists. Both documents are posted on the HQ USEUCOM Force Protection homepage on the SIPRNet.

---

(CLASSIFICATION)

**M-2-C-1**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

(CLASSIFICATION)

**VULNERABILITY ASSESSMENT CHECKLIST SITE OVERVIEW**

<b>SITE / INSTALLATION:</b>	
<b>UNIT:</b>	
<b>CONTACT PHONE NUMBERS:</b>	
<b>STU III NUMBERS:</b>	
<b>MESSAGE ADDRESS:</b>	
<b>E-MAIL ADDRESS:</b>	
<b>TERRORISM THREAT LEVEL:</b>	
<b>Force Protection Condition:</b>	
<b>TYPE OF INSTALLATION:</b>	
<b>LOCATION (Include Grid Coordinates if available):</b>	
<b>DATE OF LAST LOCAL ASSESSMENT</b>	
<b>DATE OF LAST HHQ ASSESSMENT:</b>	
<b>PREVIOUS DEFICIENCIES</b>	See TAB ____ attached (or N/A)
<b>LOCAL POCs/PHONE NUMBERS:</b>	
<b>COMMANDER:</b>	
<b>ANTITERRORISM OFFICER (ATO):</b>	
<b>FORCE PROTECTION:</b>	
<b>INTELLIGENCE:</b>	
<b>COMMUNICATIONS:</b>	
<b>INFO SECURITY:</b>	
<b>OPSEC:</b>	
<b>MEDICAL:</b>	
<b>ENGINEERING:</b>	
<b>ASSESSMENT TEAM COMPOSITION:</b>	
<b>EMARKS:</b>	

(CLASSIFICATION)

**M-2-C-2****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

(CLASSIFICATION)

#	ITEM	REMARKS (include both evaluator observations/comments and unit comments/concerns)
A.	<b>Antiterrorism/Force Protection (AT/FP) Command Relationships</b>	
1.	Does commander have operational control over all U.S. forces under his tactical command? <input type="checkbox"/> If not, what units are not under operational control	
2.	Who has operational control over this unit?	
3.	Who has tactical control (for Force Protection) over this unit?	
B	<b>Signed/executable AT/FP Plan fully coordinated with tasked units</b>	
1.	Is a comprehensive AT/FP Plan published? (It must be coordinated, signed, resourced, distributed, and exercised.) Does the Plan include the following key elements? <ul style="list-style-type: none"> <li>o a. Terrorism Threat Assessment</li> <li>o b. Vulnerability Assessment</li> <li>o c. Risk Assessment</li> <li>o d. Physical Security Measures</li> <li>o e. Terrorist Incident Response Measures</li> <li>o f. Consequence Management Measures</li> </ul>	
2.	The following should be included in the AT/FP Plan: <ul style="list-style-type: none"> <li>o a. AT/FP mission and concept of operations.</li> <li>o b. Task organization and Mission Essential or Vulnerable Areas (MEVA).</li> <li>o c. Installation Working Groups or similar organizations.</li> <li>o d. Threat assessment process and annual threat assessment including WMD.</li> <li>o e. Vulnerability assessment process and annual vulnerability assessment.</li> <li>o f. Baseline AT/FP posture.</li> <li>o g. Command, control and communications.</li> <li>o h. Risk assessment process, addressing both MEVAs and operations.</li> <li>o i. Physical Security Measures.</li> <li>o j. Implementation procedures for higher headquarters or site specific Force</li> </ul>	

(CLASSIFICATION)

**M-2-C-3****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

(CLASSIFICATION)

	<p>Protection Conditions</p> <ul style="list-style-type: none"> <li>○ k. Incident Response procedures to include First Responders and follow-up forces.</li> <li>○ l. Crisis management organization and concept of operations.</li> <li>○ m. Consequence management organization and concept of operations.</li> <li>○ n. Security Force operations (including augmentation forces) and post priorities</li> <li>○ o. Random Antiterrorism Measures (RAM).</li> <li>○ p. Barrier plans.</li> <li>○ q. Activity curtailment.</li> <li>○ r. Training.</li> <li>○ s. Exercises and Lessons Learned.</li> <li>○ t. MOUs and MOAs.</li> <li>○ u. Mass Notification Procedures.</li> <li>○ v. High Risk Personnel Protection Procedures.</li> </ul>	
3.	<p>Is Incident Response planning comprehensive to include the following requirements:</p> <ul style="list-style-type: none"> <li>○ a. Preparation for multiple incidents or diversionary tactics.</li> <li>○ b. Establishment of communications nets.</li> <li>○ c. Activation of required resources.</li> <li>○ d. Preparation for prolonged incidents.</li> <li>○ e. Management of media.</li> <li>○ f. Transition to crisis/ consequence management to include the following: <ul style="list-style-type: none"> <li>○ (1) Bombings/ explosions.</li> <li>○ (2) Bomb threats</li> <li>○ (3) Assaults/raids.</li> <li>○ (4) Kidnappings.</li> <li>○ (5) Hostage/Barricade.</li> <li>○ (6) Other probable scenarios.</li> </ul> </li> </ul>	
4.	Are there SOPs to support the AT/FP Plan?	
5.	When was the AT/FP Plan last updated?	
<b>C</b>	<b>Intelligence Support</b>	
1.	<p>Communication Architecture</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> a. How does the unit receive routine intelligence?</li> <li><input type="checkbox"/> b. How are time sensitive Indications &amp; Warnings received?</li> <li><input type="checkbox"/> c. Is unit receiving warnings via Blue Dart system?</li> <li><input type="checkbox"/> d. Does unit have procedures for rapidly</li> </ul>	

(CLASSIFICATION)

M-2-C-4

**FOR OFFICIAL USE ONLY**



## FOR OFFICIAL USE ONLY

(CLASSIFICATION)

	<p><b>processing Blue Dart warnings?</b></p> <input type="checkbox"/> e. Is there a redundant system for each in event of outage?	
2.	Does the commander/ATO have an intelligence support capability?	
<b>D.</b>	<b>Physical Security</b>	
1.	Do Physical Security measures comply with DoD 2000.12-H?	
2.	Is security in depth (concentric circles) established?	
3.	Evaluate perimeter for need/adequacy of: <ul style="list-style-type: none"> <li><input type="checkbox"/> a. Standoff Distance</li> <li><input type="checkbox"/> b. Barriers</li> <li><input type="checkbox"/> c. Entry Points</li> <li><input type="checkbox"/> d. Lighting</li> <li><input type="checkbox"/> e. Detection/Sensor Systems</li> <li><input type="checkbox"/> f. Military Working Dogs (Patrol/Explosive Detection)</li> </ul>	
4.	Evaluate adequacy of PS standards/practices for: <ul style="list-style-type: none"> <li><input type="checkbox"/> a. Aircraft</li> <li><input type="checkbox"/> b. Vehicles</li> <li><input type="checkbox"/> c. Weapons</li> <li><input type="checkbox"/> d. Ammunition</li> <li><input type="checkbox"/> e. Sensitive/High Value Items</li> <li><input type="checkbox"/> f. Command &amp; Control</li> </ul>	
5.	Mission Essential Vulnerable Areas (MEVAs) <ul style="list-style-type: none"> <li><input type="checkbox"/> a. Are periodic Risk Assessments conducted?</li> <li><input type="checkbox"/> b. Are AT/FP measures commensurate with threat/vulnerabilities?</li> </ul>	
6.	Installation Warning Systems <ul style="list-style-type: none"> <li><input type="checkbox"/> a. Are installation warning systems in place?</li> <li><input type="checkbox"/> b. Is system redundant?</li> <li><input type="checkbox"/> c. Is there an SOP for alarm use?</li> <li><input type="checkbox"/> d. What is time between threat activity being detected and general alarm being given?</li> <li><input type="checkbox"/> e. Who can activate alarm?</li> <li><input type="checkbox"/> f. Where are activation switches/buttons/etc. located?</li> </ul> <input type="checkbox"/> a. Has training been conducted for ALL	

(CLASSIFICATION)

M-2-C-5

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

	<p>who might need to use?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> (1) Is this training documented?</li> <li><input type="checkbox"/> (2) Are procedures in place/followed to train new personnel?</li> </ul> <p><input type="checkbox"/> h. Are all personnel trained to recognize and react to alarm?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> (1) Is this training documented?</li> <li><input type="checkbox"/> (2) Are procedures in place/followed to train new personnel?</li> </ul> <p><input type="checkbox"/> i. When was the last test?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> (1) What were lessons learned?</li> <li><input type="checkbox"/> (2) Were any deficiencies corrected / re-tested?</li> </ul>	
7.	Are installation access procedures established?	
8.	<p>a. Are background investigations conducted on local nationals authorized unescorted access?</p> <p>b. Is there a process established to retrieve and/or account for identification cards/badges from contractors/employees no longer associated with the DoD facility or site?</p>	
9.	<p>Industrial Safety and Environmental Concerns:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Is the unit/facility located near toxic or hazardous areas that could multiply the effects of a terrorist attack?</li> </ul>	
<b>E.</b>	<b>Information Security/ OPSEC</b>	
1.	Is classified information stored in approved containers?	
2.	Are combinations changed as required?	
3.	Are clearances and need to know verified prior to information dissemination?	
4.	Is operational information protected from unauthorized disclosure?	
5.	Are documents destroyed when no longer needed?	
6.	What procedures are followed to avoid establishing unit routines?	
7.	Do individuals avoid routines?	
<b>F.</b>	<b>AT/FP Awareness Training &amp; Education</b>	
1.	<ul style="list-style-type: none"> <li><input type="checkbox"/> a. Is structured AT/FP training conducted with all personnel?</li> <li><input type="checkbox"/> b. Is this training documented?</li> <li><input type="checkbox"/> c. Are procedures in place/followed to train new personnel?</li> </ul>	

**(CLASSIFICATION)**

**M-2-C-6**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****(CLASSIFICATION)**

2.	<input type="checkbox"/> a. Are training exercises conducted to rehearse responses to attack, including QRF responsibilities, building evacuation, and re-assembly procedures? <input type="checkbox"/> b. Last conducted: <input type="checkbox"/> c. Lessons learned:	
3.	Has JS Guide 5260 Service Member's Personal Protection Guide (or equivalent) been made available to all DoD personnel?	
4.	Is there a need to require a Residential Security survey for all DoD personnel?	
<b>G.</b>	<b>Guard Force</b>	
1.	<input type="checkbox"/> a. Is there a Guard Force SOP? <input type="checkbox"/> b. Last Reviewed	
2.	Are the guard force personnel assigned to the commander?	
3.	<input type="checkbox"/> a. Are personnel trained on procedures? <input type="checkbox"/> b. Is this training documented? <input type="checkbox"/> c. Are procedures in place/ followed to train new personnel?	
4.	Is equipment adequate: (i.e. radios, binoculars, NODs, alarms, flares, personal equipment)?	
5.	Are guard posts/towers conducive to good operations? (hardened, overhead cover, enclosed if appropriate, heated, dry, in line of sight to adjacent positions, redundant communications)	
6.	Does commander have plan and assets to implement measures for higher Force Protection Conditions?	
<b>H.</b>	<b>Quick Reaction Force (QRF)</b>	
1.	Does Commander have a QRF?	
2.	Are the QRF personnel assigned to the commander?	
3.	<input type="checkbox"/> a. Is there a QRF SOP? <input type="checkbox"/> b. Last Reviewed?	
4.	<input type="checkbox"/> a. Are personnel trained on AT/FP procedures? <input type="checkbox"/> b. Is this training documented? <input type="checkbox"/> c. Are procedures in place/ followed to	

**(CLASSIFICATION)****M-2-C-7****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****(CLASSIFICATION)**

	train new personnel?	
5.	<input type="checkbox"/> a. When was last QRF exercise? <input type="checkbox"/> b. What were lessons learned? <input type="checkbox"/> c. Were deficiencies corrected/re-tested?	
<b>I.</b>	<b>Weapons</b>	
1.	Are weapons adequate for potential threats?	
2.	Is sufficient ammunition readily available to personnel?	
3.	Have personnel zeroed their weapon(s)?	
4.	<input type="checkbox"/> a. Have personnel fired their weapons for familiarization? <input type="checkbox"/> b. Last weapons qualification?	
5.	Do weapons appear to be receiving proper maintenance?	
<b>J.</b>	<b>Less Than Lethal Weapons</b>	
1.	Are less than lethal weapons available?	
2.	If not, could unit benefit from such equipment?	
3.	Are personnel trained in proper use?	
<b>K.</b>	<b>Rules of Engagement (ROE)/Use of Deadly Force</b>	
1.	Have Rules of Engagement been established?	
2.	<input type="checkbox"/> a. Are personnel trained on ROE? <input type="checkbox"/> b. Is ROE training documented? <input type="checkbox"/> c. Are procedures in place/followed to train new personnel?	
3.	Is ROE simple, with high reliance on the judgment of individuals to make correct decisions on the spot?	
<b>L.</b>	<b>Medical Support/Mass Casualty Exercises/ Preventative Medicine</b>	
1.	Is medical support (personnel & equipment) adequate?	
2.	Are personnel required to wear identification tags at all times?	
3.	Does the military medical facility maintain an updated roster of critical medical information for each individual?	
4.	<input type="checkbox"/> a. Has unit conducted and evaluated realistic mass casualty training and exercise scenarios? <input type="checkbox"/> b. Last Conducted:	

**(CLASSIFICATION)****M-2-C-8****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****(CLASSIFICATION)**

	<input type="checkbox"/> c. Lessons Learned:	
5.	What procedures are in place to support organic medical staff in the event of a mass casualty situation?	
6.	What medical support (personnel and equipment) is available to personnel at outlying posts or on patrol (medics, combat lifesavers, etc.)?	
7.	Does unit emphasis first aid training for all personnel?	
8.	What procedures are in place to prevent/detect contamination to water supply?	
9.	What procedures are in place to prevent/detect contaminated food supplies (U.S. and locally procured)?	
10.	Have personnel received required immunizations?	
11.	Have deployable personnel been assessed and determined medically & psychologically fit for worldwide deployment?	
12.	Have deployable personnel received a medical threat briefing by unit medical personnel?	
13.	Have deployable personnel received pre-deployment briefings and pre-deployment health screenings?	
14.	Does the installation have medical personnel with preventive medicine background to teams evaluating commands, personnel and facilities?	
<b>M.</b>	<b>Transportation security</b>	
1.	Does vehicle armoring suffice for: <input type="checkbox"/> a. current threat level/ Force Protection Condition? <input type="checkbox"/> b. increased threat levels/Force Protection Conditions?	
2.	Are routines avoided?	
3.	Are there sufficient numbers of personnel trained in protective services/threat avoidance driving techniques?	

<b>N.</b>	<b>Unique security problems</b>	
1	Has vulnerability and response to unique threats been adequately addressed: <input type="checkbox"/> a. Stand-off weapons attack (e.g., mortar)? <input type="checkbox"/> b. Sniper fire?	

**(CLASSIFICATION)****M-2-C-9****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****(CLASSIFICATION)**

	<input type="checkbox"/> c. Hostile aircraft (conventional and unconventional)?	
<b>O.</b>	<b>WMD Readiness</b>	
1.	<input type="checkbox"/> Consideration of terrorist use of WMD: <input type="checkbox"/> a. Chemical attack? <input type="checkbox"/> b. Biological attack? <input type="checkbox"/> c. Nuclear/Radiological attack?	
2.	<input type="checkbox"/> Do all personnel have individual protective equipment available? <input type="checkbox"/> Masks <input type="checkbox"/> Boots <input type="checkbox"/> Gloves <input type="checkbox"/> Filters <input type="checkbox"/> Spare parts <input type="checkbox"/> Are personnel trained to use their equipment?	
3.	<input type="checkbox"/> Are collective protective systems available?	
4.	<input type="checkbox"/> What NBC detection equipment is available? <input type="checkbox"/> Is the detection equipment deployed?	
5.	<b>Does an NBC Warning and Reporting System (automated or manual) exist?</b>	
6.	Decontamination: <input type="checkbox"/> a. Is there individual decontamination available? Are personnel trained to use equipment? <input type="checkbox"/> b. Is there collective decontamination equipment? <input type="checkbox"/> c. Are there procedures to decontaminate casualties from NBC attack? <input type="checkbox"/> d. When was last time training on decontamination procedures took place?	
<b>P.</b>	<b>Integrated Technology</b>	
1.	How is technology being used to enhance security and human performance?	
2.	What technologies have been identified as recommended / required for higher threat levels/Force Protection Conditions?	
3.	What additional technologies should be considered at this or higher threat levels? (Examples: Shatter resistant window film [Mylar], heavy curtains, Kevlar curtains, blast blankets for vehicles, motion sensors, cameras, etc.)	
<b>Q.</b>	<b>Host nation support / coordination</b>	
1.	Have working relationships been established	

**(CLASSIFICATION)****M-2-C-10****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****(CLASSIFICATION)**

	and maintained between senior commanders and appropriate host nation officials?	
2.	Has planning / coordination been conducted with host nation officials concerning: <ul style="list-style-type: none"> <li><input type="checkbox"/> a. Warning in event of public health crisis?</li> <li><input type="checkbox"/> b. Warnings of potential natural emergencies (flood, severe storms, etc. Warnings of threats to U.S. forces?</li> <li><input type="checkbox"/> c. Routine security patrols outside installations?</li> <li><input type="checkbox"/> d. Host nation support in event of: <ul style="list-style-type: none"> <li><input type="checkbox"/> (1) Fire on U.S. installation?</li> <li><input type="checkbox"/> (2) Attack against U.S. forces?</li> <li><input type="checkbox"/> (3) Mass casualty situation?</li> </ul> </li> </ul>	
3.	Does commander have sufficient interpreters to support senior level interaction with host nation officials or allied forces on daily mission requirements (gates, MP/SP station, etc.) and emergency situations?	
<b>R</b>	<b>ALLIED OPERATIONS</b>	
1.	If this is a CTF, or Combined Exercise, are allied forces integrated into the AT/FP plan?	
2.	Does commander have sufficient interpreters and/or LNOs to coordinate with allied forces on daily mission requirements (gates, MP/SF station, etc.) and emergency situations?	
<b>S</b>	<b>SAFETY</b>	
1.	Is the Risk Management process integrated into planning and execution?	
2.	Are Risk Assessments completed for all operations?	
3.	Are countermeasures against greatest threats fully implemented? <ul style="list-style-type: none"> <li><input type="checkbox"/> a. fire prevention?</li> <li><input type="checkbox"/> b. vehicle accidents?</li> <li><input type="checkbox"/> c. personal injuries?</li> <li><input type="checkbox"/> d. Terrorist attack?</li> </ul>	
4.	Are pre-accident plans developed/exercised?	
5.	Are fire prevention plans developed/exercised?	
6.	<ul style="list-style-type: none"> <li><input type="checkbox"/> a. Is fire response and protection capability adequate?</li> <li><input type="checkbox"/> b. personnel?</li> <li><input type="checkbox"/> c. equipment?</li> </ul>	
7.	Is HAZMAT prevention planning and response capability adequate?	
8.	Are explosive safety requirements met?	

**(CLASSIFICATION)****M-2-C-11****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****(CLASSIFICATION)**

9.	Are range safety requirements met?	
<b>T</b>	<b>WEAPONS EFFECTS</b>	NOTE: These questions/calculations should be completed for all key buildings (large population, close to perimeter, important mission)
1.	Photographs: All sides of building, roof (inside and out), building frame (column, beams, slabs, drop panels, etc.), close up details (windows, curtain, etc.)	
2.	Construction Type: Frame type (load bearing walls, steel frame, etc.), window type, number of floors, floor materials, roof materials, wall materials, use (barracks, office, warehouse)	
3.	Window Information: Window material, thickness, size, calculated hardness (psi)	
4.	Weakest Roof Panel Information: Overall roof dimensions, roof panel dimensions, description of construction, roof structural material information, calculated hardness (psi)	
5.	Weakest Wall Information (each major face): Wall dimensions, thickness, description of construction, wall structural material information, calculated hardness (psi)	
6.	Frame Information: Dimensions of floor system, spans, description of construction, structural material information, calculated hardness (psi)	
<b>U</b>	<b>RED FORCE</b>	
1.	OPERATIONAL INTELLIGENCE COLLECTION	
a.	Installation Description. Primary mission, unit ID/mission, estimate of installation population, map, installation imagery, locate probable population centers, determine occupancy by time, composition & numbers, Data on key personnel, ID locations for covered OP's, locate possible infiltration/egress routes, installation/local area pubs (papers, bulletins, phone lists)	
b.	Surrounding Area. Commercial roads near perimeter, point of closest approach to perimeter, number & location of approaches to installation, high speed approaches, freq. & type - LEA patrols	
2.	ACCESS ASSESSMENT	

**(CLASSIFICATION)****M-2-C-12****FOR OFFICIAL USE ONLY**



**FOR OFFICIAL USE ONLY****(CLASSIFICATION)**

a	Perimeter Adjacent Area. Clear zone, external perimeter patrol road (signs of use), access denial devices (mines, electric fence), buried/above ground sensors, cameras, drainage/utility access	
b	Perimeter Barriers Type/size, obstacles on perimeter barrier (razor tape, other), fence line anchoring (stakes or poured sill, sensors/alarms, sensor type, cameras (dead space), lighting, perimeter weaknesses, proximity to roads, cover/concealment	
c	Vehicle Entry Points. Vehicle barriers (type, construction, psn), gates, location/type entrapment area, inspection areas, access limits (vehicle size, #), hours of peak inbound traffic, hours of peak outbound traffic, gate/entrapment ops during peak traffic hours, hours of operation for each gate, limits of movement w/in installation, ID requirements, vehicle search (exemptions)	
d	Personnel Entry Points. Personnel barriers (type, construction, psn), gates, location/type entrapment area, access limits (vehicle size, #), hours of peak inbound traffic, hours of peak outbound traffic, gate/entrapment ops during peak traffic hours, hours of operation for each gate, limits of movement w/in installation, ID requirements, personnel search (exemptions)	
e	Guard Force. Composition by shift, time of shift change, rotation/ breaks, manning at fixed (ECP, OP), manning of mobile assets (patrols), probable location & # of unobserved guards, location of crew served/heavy weapons, proximity of HN support forces.	

**(CLASSIFICATION)****M-2-C-13****FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

---

**(CLASSIFICATION)**

f	Population Concentration. Area/Bldg #/location: function, VIP offices, construction type, peak occupancy hours, est. max occupancy, surrounding area, security (REPEAT FOR ADDITIONAL AREAS/BLDGS)	
g	Infiltration/Egress Routes. Overt entry & exit, covert entry, covert exit. (both vehicle and pedestrian.	
h	Destructive Mechanism.  TARGET SELECTION: <input type="checkbox"/> potential for MASCAL <input type="checkbox"/> ease of access <input type="checkbox"/> probability of success <input type="checkbox"/> probability of escape <input type="checkbox"/> local threat  WEAPONS SELECTION: <input type="checkbox"/> target construction <input type="checkbox"/> target access <input type="checkbox"/> threat tech capabilities	

**Additional Notes:**

---

**(CLASSIFICATION)****M-2-C-14****FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### **TAB D (ASSESSMENT/SURVEY CHECKLISTS) TO APPENDIX 2 (VULNERABILITY ASSESSMENTS AND PROGRAM REVIEWS) TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPO RD 01-01**

1. The following three checklists are included to provide users of this OPO RD a resource with which to conduct detailed assessments of installation/activity/facility vulnerabilities. These checklists are designed as guides, which users may and should modify for their own use.

a. The first checklist, General Physical Security Checklist, is designed to assist in conducting vulnerability assessments of installations and facilities. It focuses on the collection of detailed physical security data to support assessments using the checklist in Tab C of this Appendix.

b. The second, Survey Checklist For Residential Security and Personal Security Practices, is designed to assist in evaluating both off-installation and on-installation residences as well as the personal security practices of individuals and family members.

c. The third, 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. DoD Handbook 2000.12-H provides additional checklists for various other types of facilities.

**M-2-D-1**

**FOR OFFICIAL USE ONLY**

# FOR OFFICIAL USE ONLY

(CLASSIFICATION)

## General Physical Security CHECKLIST

<b>A. GENERAL</b>			
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:			
<input type="checkbox"/> (a) Compass rose showing north			
<input type="checkbox"/> (b) All existing buildings and their function, all interior and exterior roads, all fences, and other physical barriers			
<input type="checkbox"/> (c) Railroad sidings or main track			
<input type="checkbox"/> (d) Airfield facilities including runways, taxiways, helipads, supporting utilities, or utilities lying beneath such surfaces			
<input type="checkbox"/> (e) Location of gates (active and inactive)			
<input type="checkbox"/> (f) Parking lots/areas, and types of personnel using them			
<input type="checkbox"/> (g) Any planned remodeling or expansion of facilities.			
6. Obtain as-built drawing of the office or residential structure showing:			
<input type="checkbox"/> (a) Construction of exterior and interior walls			
<input type="checkbox"/> (b) Location of all windows, doors, and skylights			
<input type="checkbox"/> (c) Location and size of all vents, utility openings, other building penetrations			
<input type="checkbox"/> (d) Electrical runs, outlets, and switches for all voltages.			
7. Location of facility (check as applicable and describe)			
<input type="checkbox"/> Urban			
<input type="checkbox"/> Suburban			
<input type="checkbox"/> Incorporated			
<input type="checkbox"/> Unincorporated			
<input type="checkbox"/> Government Installation			

(CLASSIFICATION)

M-2-D-2

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

Socioeconomic environment (check one, describe)			
<input type="checkbox"/> Residential			
<input type="checkbox"/> Industrial			
<input type="checkbox"/> Commercial			
<input type="checkbox"/> Agricultural			
(a) Neighboring area is: <input type="checkbox"/> Affluent <input type="checkbox"/> Middle Class <input type="checkbox"/> Poor			
(b) Comments:			
9. Area crime rate: <input type="checkbox"/> High <input type="checkbox"/> Moderate <input type="checkbox"/> 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? <input type="checkbox"/> Yes <input type="checkbox"/> No			
12. Is there an active security awareness program? <input type="checkbox"/> Yes <input type="checkbox"/> No			
13. Number of employees			
14. Are background investigations conducted prior to 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:			

**(CLASSIFICATION)**

# FOR OFFICIAL USE ONLY

(CLASSIFICATION)

<b>B. PERIMETER SECURITY</b>
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 which 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 step ladder 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?

(CLASSIFICATION)

M-2-D-4

# FOR OFFICIAL USE ONLY

---

## (CLASSIFICATION)

(h) Are gates which 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 which 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:
<b>C. PERIMETER LOCK SYSTEM</b>
1. Locks
(a) What type of locks are used?
(b) Name of manufacturer
(c) Are cylinders removable? <input type="checkbox"/> Yes <input type="checkbox"/> No
(d) Are locks changed when security may be compromised? <input type="checkbox"/> Yes <input type="checkbox"/> 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? <input type="checkbox"/> Yes <input type="checkbox"/> No
(2) Case hardened chains? <input type="checkbox"/> Yes <input type="checkbox"/> No
(i) Are all lock numbers recorded? <input type="checkbox"/> Yes <input type="checkbox"/> No
(j) Are numbers obliterated? <input type="checkbox"/> Yes <input type="checkbox"/> No

---

## (CLASSIFICATION)

**M-2-D-5**

# FOR OFFICIAL USE ONLY

(CLASSIFICATION)

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	
<b>D. PERIMETER ALARM SYSTEMS</b>	
1. Perimeter alarms	
(a) Are perimeter alarms employed? <input type="checkbox"/> Yes <input type="checkbox"/> No	
(1) Manufacturer	
(2) Is the alarm: Local <input type="checkbox"/> Yes <input type="checkbox"/> No	
Central Station <input type="checkbox"/> Yes <input type="checkbox"/> No	
Silent <input type="checkbox"/> Yes <input type="checkbox"/> No	
Direct (Police) <input type="checkbox"/> Yes <input type="checkbox"/> 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? <input type="checkbox"/> Yes <input type="checkbox"/> No	
(b) If a perimeter alarm detector is used, does restoring door or window to original position stop alarm? <input type="checkbox"/> Yes <input type="checkbox"/> No	
(c) Does alarm have a battery back-up	<input type="checkbox"/> Yes <input type="checkbox"/> No
(d) Is battery checked periodically for suitable charge	<input type="checkbox"/> Yes <input type="checkbox"/> No
(e) Are duress alarms used at any point?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6. Comments	
<b>E. PERIMETER LIGHTING</b>	
1. Are all perimeter areas lighted during hours of darkness <input type="checkbox"/> Yes <input type="checkbox"/> 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? <input type="checkbox"/> Yes <input type="checkbox"/> No	
Exceptions	
5. Does perimeter lighting also cover the buildings? <input type="checkbox"/> Yes <input type="checkbox"/> No	
6. If lights burn out, do light patterns overlap? <input type="checkbox"/> Yes <input type="checkbox"/> No	
7. Is someone responsible for turning lights on and off? <input type="checkbox"/> Yes <input type="checkbox"/> No	
(a) If so, whom?	

(CLASSIFICATION)

M-2-D-6



# FOR OFFICIAL USE ONLY

(CLASSIFICATION)

(b) Who is responsible for lighting maintenance?	
(c) Are there adequate supplies on hand for maintenance of lighting system (bulbs, fuses, etc.) <input type="checkbox"/> Yes <input type="checkbox"/> 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	
<b>F. GUARD SERVICE</b>	
1. Is a guard service employed? <input type="checkbox"/> Yes <input type="checkbox"/> No	
<input type="checkbox"/> Contractor <input type="checkbox"/> US Military	
<input type="checkbox"/> Foreign Military <input type="checkbox"/> 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? <input type="checkbox"/> Yes <input type="checkbox"/> No	
4. Are guards free from "extra duties" so they are able to perform their protective duties? <input type="checkbox"/> Yes <input type="checkbox"/> 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? <input type="checkbox"/> Yes <input type="checkbox"/> No	
(a) How often?	
(b) Who gives them?	

(CLASSIFICATION)

M-2-D-7

# FOR OFFICIAL USE ONLY

(CLASSIFICATION)

13. What type of communication system is used? (Primary "P", Backup "B")		
Telephone		
Radio		
Pak sets		
Alarm switch		
14. Comments		
<b>G. INTERIOR</b>		
(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: <input type="checkbox"/> Wood <input type="checkbox"/> 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 window panes 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 use?		
<b>H. OBSCURE OPENINGS</b>		
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:		
<b>I. OFFICE OPERATIONS/ACCESS CONTROL</b>		
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?		

(CLASSIFICATION)

M-2-D-8

# FOR OFFICIAL USE ONLY

(CLASSIFICATION)

(1) Controlled by:
<input type="checkbox"/> Badge
<input type="checkbox"/> Pass
<input type="checkbox"/> Guard
<input type="checkbox"/> Key
<input type="checkbox"/> Receptionist
(b) Do all employees have badges?
(c) Do employees wear ID badges with pictures on them? <input type="checkbox"/> Yes <input type="checkbox"/> No
(d) Is the egress/ingress control point used for employees the same as the one used for visitors, vendors, repairmen, etc.? <input type="checkbox"/> Yes <input type="checkbox"/> No
4. Who opens in the morning?
5. Who closes in the evening?
6. Comments
<b>J. PARKING</b>
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
<b>K. KEY CONTROL</b>
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

(CLASSIFICATION)

M-2-D-9

# FOR OFFICIAL USE ONLY

(CLASSIFICATION)

<b>L. VENDOR AND VISITOR CONTROL</b>
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.?
<input type="checkbox"/> Yes <input type="checkbox"/> No
5. Is a property pass system used for property removal? <input type="checkbox"/> Yes <input type="checkbox"/> No
6. Comments
<b>M. CONTRACT PERSONNEL</b>
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)
<b>NAME &amp; ADDRESS</b>
<b>TYPE OF WORK</b>
(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 which enter the facility have an identifying decal?
(d) Are the vehicles of contractors inspected?
(e) Is there an identification system for contractors?
3. Comments
<b>N. DISPOSAL</b>
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
<b>O. EMERGENCY PLANS</b>
1. Does the facility have emergency plans?

(CLASSIFICATION)

M-2-D-10

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

(a) Bomb Threat	<input type="checkbox"/> Yes <input type="checkbox"/> No
(b) Fire	<input type="checkbox"/> Yes <input type="checkbox"/> No
(c) Tornado	<input type="checkbox"/> Yes <input type="checkbox"/> No
(d) Hurricane	<input type="checkbox"/> Yes <input type="checkbox"/> No
(e) Flood	<input type="checkbox"/> Yes <input type="checkbox"/> No
(f) Earthquake	<input type="checkbox"/> Yes <input type="checkbox"/> No
(g) Explosion	<input type="checkbox"/> Yes <input type="checkbox"/> No
(h) Loss of utility service	<input type="checkbox"/> Yes <input type="checkbox"/> No
(i) Civil disorder	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>2. Personnel safety</b>	
(a) Safety supervisor	
(b) Are safety plans posted?	
(1) Up-to-date?	
(2) Clear and concise	
3. Is there an Emergency Plan Coordinator? <input type="checkbox"/>	Name
Yes <input type="checkbox"/> No	
4. Has the plan been tested? <input type="checkbox"/> Yes <input type="checkbox"/> No	
When?	
5. Are drills conducted? <input type="checkbox"/> Yes <input type="checkbox"/> No	
6. Comments	
<b>P. OFFICE</b>	
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	
<b>Q. ALARM SYSTEMS</b>	
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?	
<b>R. MISCELLANEOUS</b>	
1. Are buildings locked at night?	
(a) Who is responsible?	

**(CLASSIFICATION)**

**FOR OFFICIAL USE ONLY**

---

**(CLASSIFICATION)**

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:

---

**(CLASSIFICATION)**

**M-2-D-12**

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

**SURVEY CHECKLIST FOR RESIDENTIAL SECURITY  
AND PERSONAL SECURITY PRACTICES**

<b>Area</b>	<b>Yes</b>	<b>No</b>	<b>Remarks</b>
<b>A. GENERAL</b>			
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>B. EXTERIOR</b>			
1. Is exterior lighting checked			

**(CLASSIFICATION)**

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

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?			
<b>C. BUILDING</b>			
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			

**(CLASSIFICATION)**



**FOR OFFICIAL USE ONLY**

---

**(CLASSIFICATION)**

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			

---

**(CLASSIFICATION)**

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

roof doors properly secured?			
35. Is outside security lighting adequate?			
36. Are there lights to illuminate the sides of the residence, parking area and entrance way?			
37. Does the main entrance to the apartment complex remain secured when not in use?			
38. Does the apartment require a burglar alarm?			
<b>D. SECURITY PROCEDURES</b>			
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 house-sit 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?			
<b>E. SAFEHAVEN</b>			
1. Does safehaven 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?			

**(CLASSIFICATION)**

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

(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?			
<b>F. PERSONAL SECURITY PRACTICES</b>		<b>YES</b>	<b>NO</b>
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.)			

**(CLASSIFICATION)**

## FOR OFFICIAL USE ONLY

(CLASSIFICATION)

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 prior to 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.		
<b>NOTE:</b> 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.		

(CLASSIFICATION)

M-2-D-18

# FOR OFFICIAL USE ONLY

(CLASSIFICATION)

## SECURITY SURVEY WORKSHEET FOR HIGH-RISE COMMERCIAL BUILDINGS

Area	Yes	No	Remarks
<b>A. PRE-SURVEY INFORMATION AND MATERIAL TO BE OBTAINED</b>			
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>B. SECURITY AT STREET LEVEL AND BELOW</b>			
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			

(CLASSIFICATION)

M-2-D-19

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

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?			
<b>C. LOBBY</b>			
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?			

**(CLASSIFICATION)**

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

(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			

**(CLASSIFICATION)**

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

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?			
<b>3. Custodial personnel</b>			
(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?			
<b>D. BUSINESS FIRMS IN THE BUILDING</b>			
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			

**(CLASSIFICATION)**



**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

parts of it are closed?			
5. Are there any businesses or professional offices which 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?			
<b>E. BASEMENTS, SUB-BASEMENTS, AND PARKING</b>			
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?			
<b>F. ROOF AREAS</b>			
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?			

**(CLASSIFICATION)**

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

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?			
<b>G. FIRE PROTECTION</b>			
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 which have no automatic protection.			
6. How many risers feed the sprinkler systems?			
7. Are the risers equipped with waterflow 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			

**(CLASSIFICATION)**

**FOR OFFICIAL USE ONLY**

**(CLASSIFICATION)**

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 pullboxes 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 fire walls 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) which would activate if a fire occurred?			

**(CLASSIFICATION)**

# FOR OFFICIAL USE ONLY

(CLASSIFICATION)

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 which would effectively block fire from spreading to other floors?			
37. Are air conditioning and ventilating flues equipped with dampers which 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,			

(CLASSIFICATION)

**FOR OFFICIAL USE ONLY**

---

**(CLASSIFICATION)**

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 they can easily be located by tenants during a fire?			

**ADDITIONAL NOTES:**

---

**(CLASSIFICATION)**

**FOR OFFICIAL USE ONLY**

---

**(CLASSIFICATION)**

**(INTENTIONALLY BLANK)**

---

**(CLASSIFICATION)**

**M-2-D-28**

## FOR OFFICIAL USE ONLY

### APPENDIX 3 (HIGH-RISK PERSONNEL) TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPOD 01-01

#### REFERENCES: See Basic Order

**1. SITUATION.** Terrorist acts should be considered as a distinct possibility when planning visits of high-ranking personnel to the USEUCOM AOR as well as the travel of USEUCOM high ranking personnel within the AOR. Planning visits, hosting, and safeguarding these officials is essential to the success of the USEUCOM mission and is a clear demonstration of America's positive presence.

**2. MISSION.** To provide definitive guidance to ensure individuals designated as "High Risk Personnel" or serving in designated "High Risk Billets" are provided an appropriate level of protection within the USEUCOM AOR.

#### **3. EXECUTION**

**a. Scheme of support.** Personnel may be designated high risk based on assignment to a high-risk billet or based on personal factors, regardless of position. Examples of the former include senior general officers serving in prominent positions who could serve as symbolic targets for terrorist attack and U.S. military personnel of all ranks operating in area where there is an active insurgency or frequent anti-U.S./NATO violence. There are two levels of High-Risk Personnel (HRP):

**(1) LEVEL 1.** HRP who have such a significantly high potential as terrorist or criminal targets as to warrant assignment of full-time protective services. This would include long-term protective services based on assignment location, or short-term protective services based on a specific threat.

**(2) LEVEL 2.** HRP who do not warrant assignment of full-time protective services but require such additional office, residential, and travel security measures as deemed appropriate based on local conditions.

**b. Tasks to subordinate units.** Commanders at each echelon will follow the following guidance as appropriate to ensure the safety and security of individuals designated as HRP or assigned to high-risk billets.

**(1) DESIGNATION OF HRP.** Use Service guidelines to determine who may make such designations. The DCINCEUR will make any such designations for DoD personnel and family members in the USEUCOM AOR who are not assigned to component commands. For personnel visiting the USEUCOM AOR, a general or flag officer in the chain of command of the hosting unit will make such determination. In the absence of a hosting unit, the USDR will make this determination.

## FOR OFFICIAL USE ONLY

**(2) VISIT PREPARATION.** Key elements to ensure HRP security and safety are executed through visit preparation and careful control of travel itinerary details. Training specific to HRP and their protection is found in Annex M, Appendix 5.

**(a)** In the absence of a hosting unit, when notified of an impending HRP visit, the USDR should consider HRP personal protection. The USDR should establish immediate contact with the U.S. Embassy RSO and advise the RSO of the impending visit. The USDR should designate a security POC for HRP visits to facilitate coordination. The type of protection requested or desired by the HRP must first be ascertained (full protection, minimal, high profile, low profile, etc.). Request all host nation security assistance through the RSO. Experience has shown host nation agencies receiving distinguished visitors do not necessarily initiate protective security measures as a matter of course. Therefore, make requests for such support through RSO channels.

**(b)** If the USEUCOM host activity is responsible for arranging proper security, do the following:

<input type="checkbox"/> (1) Determine if there is a high threat requiring special protective measures. <b>If the threat is not high, then:</b>
<input type="checkbox"/> Obtain secure accommodations.
<input type="checkbox"/> Obtain driver and vehicle.
<input type="checkbox"/> Request host nation security forces to provide security while the HRP are traveling, in quarters, visiting locations, and at social occasions. If the HRP are using their own aircraft, ask for security to be provided for the aircraft.
<input type="checkbox"/> Personal Security Operations for USCINCEUR and DCINCEUR travel is the responsibility of their assigned Protective Services Detail (PSD) who will coordinate transportation and lodging security measures.
<input type="checkbox"/> (2) If the threat is high, ensure HRP are informed of the threat so that changes to the trip itinerary can be made, if appropriate. If travel deemed appropriate, then:
<input type="checkbox"/> Recommend through HRP's command/detachment the employment of U.S. security agents to assist in security operations.
<input type="checkbox"/> If U.S. security agents are used, conduct protective service operations in accordance with applicable DoD and service regulations.
<input type="checkbox"/> If U.S. security agents are not used, the host must arrange security for the HRP. Tab B to this Appendix contains a basic security checklist.

### c. Coordinating instructions

**(1) Control of information related to HRP visits/itineraries.** The vulnerability of HRP can be reduced by restricting access to their travel plans. Control access to itineraries and other specific travel information to the maximum extent practical to protect the HRP and prevent incidents. It is recognized travel must be coordinated with host governments, arrangements made for billeting, messing, and transportation, as well as other actions taken to facilitate passage of personnel and their baggage through customs and airport security.



## FOR OFFICIAL USE ONLY

**(2) Classification of Itinerary.** Detailed travel itineraries of all HRP traveling anywhere within the USEUCOM AOR will be marked and handled as FOR OFFICIAL USE ONLY (FOUO) as a minimum. Composite itineraries which contain complete schedules with arrival/departure times and places, motorcade information, flight numbers or detailed billeting information are to be classified. Treat and carefully control separate extracts, and portions of the itinerary used to coordinate the visit as FOUO. In implementing the above guidance, the key words are “detailed travel itineraries” as opposed to limited extracts. Desk calendars, scheduled meetings, partial itineraries, and announced appearances do not have to be classified unless there is a specific threat to the HRP, location, or event.

**(3)** For “unclassified” schedules or portions of itineraries for HRP, take precautions to avoid release of information earlier than necessary. Limit dissemination of details to those who have a need-to-know and protect the FOUO information. Where available, use secure voice when HRP visit details are discussed by telephone. In some instances, face-to-face coordination of visit arrangements are preferred to written notification of sensitive details.

**(4)** The necessity for release of HRP visit information to certain host nation agencies is recognized. However, make every effort to limit dissemination to those agencies directly supporting the HRP visit. Further, the intent of this policy is to limit the ability of terrorist to obtain information on an itinerary far enough in advance to plan an attack. Consequently, do not release information to host nation prematurely. Rather, necessary information should be released as late as practical for the circumstances unique to each country. Finally, the USDR should solicit the host nation to consider security in disseminating HRP travel information.

**(5)** Although all-inclusive rules to fit every occasion are impractical, the following conditions generally increase the need to classify an itinerary:

<input type="checkbox"/> Receipt of specific threat information.
<input type="checkbox"/> Extensive HRP involvement in non-U.S. sponsored activities.
<input type="checkbox"/> HRP attendance at highly publicized or high profile events.
<input type="checkbox"/> Availability of information well before the visit.
<input type="checkbox"/> Production of HRP schedules that provide detailed information covering several days' activities.

**FOR OFFICIAL USE ONLY**

**ACKNOWLEDGE:**

**JOSEPH W. RALSTON**  
**General, USAF**

**TABS:**

- A. High-Risk Personnel Transportation Request
- B. High-Risk Personnel Security Checklist
- C. Non-Tactical Armored Vehicle Program

## FOR OFFICIAL USE ONLY

### TAB A (HIGH-RISK PERSONNEL TRANSPORTATION SUPPORT) TO APPENDIX 3 (HIGH RISK PERSONNEL) TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPORD 01-01

#### REFERENCES: See Basic Order

1. The SECDEF has authorized USCINCEUR to provide government transportation support to personnel in areas outside the United States if it is determined that public or private transportation in such areas is unsafe or not available. This authority has been further delegated, with JCS approval, to the Deputy USCINCEUR (DCINCEUR). Justification packets are required to support DCINCEUR's determination concerning safety of public or private transportation.

2. Service Secretaries have authority to grant authorizations for domicile-to-duty (or home-to-work) travel, but not for the use of government transportation for unofficial travel. Domicile-to-duty transportation authorization requests for military and DoD civilians assigned, attached, OPCON or ADCON to USAREUR/7<sup>th</sup> Army, USAFE, USNAVEUR, and MARFOREUR will be processed through service channels.

3. All requests for the use of government transportation for unofficial travel and justification packets concerning personnel assigned in the USEUCOM AOR will be made to the DCINCEUR. Requests for domicile-to-duty will be directed to the appropriate Service secretary through a component command unless the requester is directly assigned to HQ USEUCOM or a DOD element. The following documentation should be part of a justification packet:

a. Memorandum requesting that the individual(s) be authorized the use of government transportation for unofficial travel. Address the memorandum thru: HQ USEUCOM/ECSM, ATTN: (Identify POC), Unit 30400, APO AE 09131 and to: DCINCEUR, Unit 30400, APO AE 09131. Include the following information:

(1) Name, rank, branch of service, and duty position of individual.
(2) Detailed conditions that make government transportation support necessary, including a statement as to why privately owned vehicles or public transportation cannot be used and/or do not provide adequate security.
(3) Number and type (non-armored/fully armored/lightly armored) of government vehicles used to support individual. Indicate if vehicle will be used by more than one high-risk individual and estimate percentage of use devoted to this individual.
(4) Type of armored vehicle if applicable (heavy/light).
(5) Communications equipment in vehicle (radio/cellular phone/duress alarm).
(6) Whether individual will have driver or will he/she drive vehicle.
(7) All antiterrorism or evasive driving courses that vehicle operator has attended and month/year of training.
(8) Other security measures used at residence and work location (should be included in PSVA).
(9) State whether or not a protective services detail or personal security

## FOR OFFICIAL USE ONLY

officer/bodyguard is provided and by what agency (CID/MP/AFOSI/NCIS/local authorities/etc.).
--

**b.** Recent terrorist threat assessment concerning the individual(s) for whom this authority is being requested. This is usually prepared by local Military Intelligence (Army), AFOSI (Air Force), NCIS (Navy / Marine), Regional Security Officer (Embassy) or Defense Attaché Office (Embassy).

**c.** A **CID/MI** Personal Security Vulnerability Assessment (PSVA), AFOSI Protective Threat Assessment (PTA), or NCIS Personal Vulnerability Assessment (PVA) is the cornerstone for the evaluation of a comprehensive security program and is required to be conducted for the individual(s) for whom this authority is being requested. The purpose of any of the service's vulnerability assessments is to evaluate the threat to an individual from acts of terrorism and to recommend security measures that are necessary to provide the individual with protection commensurate with that threat. Due to the required enclosures and sensitive nature concerning the security measures employed and the potential for harm to these high-risk personnel, classify justification packets appropriately.

**d.** The mailing address for requests/justification packets is:

HQ USEUCOM / ECSM  
UNIT 30400  
ATTN: (Identify POC)  
APO AE 09131  
DSN Phone: 430-5037  
Commercial Phone: (49) 711-680-5037

### EXHIBITS:

1. Sample Request for Authority to Use Government Transportation for Unofficial Travel

**FOR OFFICIAL USE ONLY**

**EXHIBIT 1 TO TAB A (HIGH RISK PERSONNEL TRANSPORTATION SUPPORT) TO  
APPENDIX 3 (HIGH RISK PERSONNEL) TO ANNEX M (PHYSICAL SECURITY) TO  
USCINCEUR AT/FP OPOD 01-01**

**SAMPLE REQUEST FOR AUTHORITY TO USE GOVERNMENT TRANSPORTATION  
FOR UNOFFICIAL TRAVEL  
(Requests should be classified when appropriate.)**

**UNIT LETTERHEAD**

Date

MEMORANDUM THRU HQ USEUCOM Attn: ECSM, Unit 30400, Box 1000  
APO AE 09128

FOR Deputy Commander in Chief, US European Command, APO AE 09128

SUBJECT: Request for Authority to Use Government Transportation for Unofficial  
Travel

1. Request Major General Smith, John Q., U.S. Army, Deputy Commander xxxxxxxx, APO AE xxxxx, be designated a "High-Risk Person" and authorized the use of government transportation for unofficial travel. The following information is provided in support of this request:

a. MG Smith's residence is located approximately (distance) from (installation) which is his normal place of duty. A security assessment was conducted for MG Smith during (month/year). This assessment evaluated the threat to MG Smith from acts of terrorism and recommended security measures that are necessary to provide him with protection commensurate with that threat. One of the recommendations was that MG Smith be provided a government vehicle and driver trained in evasive driving for all travel in the local area, to include the commute between his residence and duty location.

b. A (fully armored - or lightly armored - or an unarmored) vehicle is dedicated to support the (duty position). The vehicle is equipped with (two way FM radio, cellular phone, etc.). The primary operator attended (name of evasive driver training) in (month / year). - or - The primary operator is scheduled to attend (name of evasive driver training) in (month / year).

c. A (CID/AFOSI/NCIS/MP/SF/etc.) detail provides security for MG Smith while traveling.

**M-3-A-1-1  
FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

- or -

c. MG Smith's security program does not include a protective service detail or bodyguard.

d. Residence security includes:

e. Office security includes:

2. MG Smith has been advised that the use of government transportation for unofficial travel may result in a tax liability; and that the use of U.S. government vehicles for commuting (home to work) is always a taxable fringe benefit - even when provided as part of a security program.

3. A terrorist threat assessment concerning MG Smith, dated xx XXX xx, and a copy of the security assessment report are provided as enclosures.

4. POC for this request is (include rank, name, duty position, DSN Phone, commercial phone, and fax number). Plain language message address for MG Smith's office is xxxxxx.

2 Encls

- 1. Threat Assessment
- 2. Security Assessment

SIGNATURE BLOCK

## FOR OFFICIAL USE ONLY

### TAB B (HIGH RISK PERSONNEL SECURITY SUPPORT) TO APPENDIX 3 (HIGH RISK PERSONNEL) TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPO RD 01-01

1. **GENERAL.** The following generic HRP Security Checklist should be adapted to your local conditions and used when supporting HRP visits. It is divided into three phases: notification, planning, and the visit.

#### 2. NOTIFICATION

a. Determine:

<input type="checkbox"/> (1) Name of HRP.
<input type="checkbox"/> (2) Dates of anticipated visit.
<input type="checkbox"/> (3) Mode of travel
<input type="checkbox"/> (4) Personnel accompanying HRP.
<input type="checkbox"/> (5) Anticipated itineraries of HRP and accompanying personnel (prior to visit, during visit, just after visit). Mark/handle all itineraries as FOUO material.
<input type="checkbox"/> (6) Dignitaries HRP will be visiting (working and social events).
<input type="checkbox"/> (7) Special security considerations, if any.
<input type="checkbox"/> (8) Special medical concerns of the HRP, if any.

b. Advise HRP if threat level is rated Significant or High. If warranted, recommend trip be canceled or rescheduled. If trip must take place, recommend U.S. security agents assist in security planning and monitoring operations.

#### 3. PLANNING

a. HRP hotel checklist

<input type="checkbox"/> (1) Coordinate and establish working relationship with hotel manager and/or owner.
<input type="checkbox"/> (2) Coordinate and establish working relationship with hotel security (if any).
<input type="checkbox"/> (3) Select HRP accommodations.
<input type="checkbox"/> (4) Make physical security survey of accommodations and adjacent rooms (coordinate with country RSO on the latest terrorist/criminal threat briefing).
<input type="checkbox"/> (5) Ensure rooms over, under, and adjacent to the HRP are occupied by responsible personnel. Conduct name checks if necessary.
<input type="checkbox"/> (6) Make room assignments for HRP staff.
<input type="checkbox"/> (7) Make room assignments for HRP security team personnel (if any).
<input type="checkbox"/> (8) Make arrangements for HRP accommodations key control.
<input type="checkbox"/> (9) Arrange for physical security sweep of accommodations prior to HRP arrival and continually during stay.
<input type="checkbox"/> (10) Arrange for room service, mail, gift and package delivery to be screened for explosive devices prior to being delivered to HRP.

M-3-B-1

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

<input type="checkbox"/> (11) Establish the reliability of all people who will prepare food or provide personal service for the HRP.
<input type="checkbox"/> (12) Survey fire equipment and local fire department capabilities. Don't billet HRP on a floor local fire department assets can't reach.
<input type="checkbox"/> (13) Coordinate and establish working relationship with local authorities (police, state security, etc.)
<input type="checkbox"/> (14) Inspect elevators, noting elevator capacity. Obtain elevator keys that enable the operator to by-pass floors.
<input type="checkbox"/> (15) Plan emergency escape routes from VIP accommodations. Secure all exit doors located on HRP floor, allowing a safe exit while preventing unauthorized entry.
<input type="checkbox"/> (16) Arrange for HRP baggage handling, delivery and security within the hotel.
<input type="checkbox"/> (17) Establish seating arrangements in hotel restaurant.
<input type="checkbox"/> (18) Identify room suitable for private meetings, if required. Do not use HRP accommodations.
<input type="checkbox"/> (19) Coordinate with media representatives; establish system of identification for reporters assigned to cover HRP, establish point of contact for media.
<input type="checkbox"/> (20) Establish normal exit and entry routes for HRP movement and vary which is used, on a random basis.
<input type="checkbox"/> (21) Survey possible HRP surveillance viewing positions in the surrounding buildings and areas. Coordinate with local hospitals for trauma capabilities, helicopter support and blood supplies.
<input type="checkbox"/> (22) Develop a list of 24-hour emergency telephone numbers to include:
<input type="checkbox"/> (a) Local security.
<input type="checkbox"/> (b) Fire department.
<input type="checkbox"/> (c) Ambulance service.
<input type="checkbox"/> (d) Hospital emergency rooms.
<input type="checkbox"/> (23) If HRP is accompanied by family, develop contacts for the following areas:
<input type="checkbox"/> (a) Tour guide services.
<input type="checkbox"/> (b) Shopping guide information and delivery services.
<input type="checkbox"/> (c) Recreational information.
<input type="checkbox"/> (d) Physical protection.

**b. HRP Baggage Security.** If the HRP is to arrive or depart from an airport or other transportation facility, the problem of obtaining the HRP's baggage (and that of his entourage) becomes a security matter. Baggage is generally handled without a great deal of security. Since the baggage will be delivered to or will accompany the HRP, it represents an area of vulnerability to attack.

<input type="checkbox"/> (1) Coordinate well in advance with the airport for the pickup of all party baggage.
<input type="checkbox"/> (2) Report all missing bags and provide descriptions to the air carrier to initiate a tracing action.
<input type="checkbox"/> (3) Request airport security to x-ray or examine any item of baggage which shows

**M-3-B-2**  
**FOR OFFICIAL USE ONLY**



## FOR OFFICIAL USE ONLY

signs of tampering or which is found to be unlocked or altered.

- (4) Drive all HRP party baggage to destination hotel and directly supervise the hand delivery of each bag to its owner. Let the bellboy move the baggage on his cart, but remain with him during all deliveries. Do not leave any baggage unattended. Ensure all baggage has valid identification markings prior to room deliver.

**c. HRP Aircraft Security.** Frequently the HRP will arrive in their own aircraft. Security arrangements for the aircraft and crew will generally be required.

- (1) Contact local authorities to request security for the aircraft. This includes a secure aircraft parking location and 24-hour guards, who are designated solely for the HRP's aircraft.
- (2) Arrange method by which the air crew can freely access the aircraft as needed.
- (3) Should the HRP bring his own security, arrange for flight line access, transportation for shift changes, health and comfort items.

### **d. HRP Automobile Travel and Route Security**

- (1) Select multiple routes of travel in conjunction with local authorities.
- (2) Acquire street maps covering the movement routes.
- (3) Drive the entire movement route at the same time of day the VIP will be traveling, on the same day of the week if possible -- *Develop a time and distance driving log for the entire travel route.*
- (4) Identify roadway and/or traffic flow choke points along the route of travel which cause excessive slowing or frequent stopping of the HRP vehicle.
- (5) Coordinate with local authorities; explain choke point problems associated with HRP movement and attempt to modify route of travel, or secure assignment of police officers to guide or control traffic flow.
- (6) Arrange for escort vehicles if required.
- (7) Arrange for a vehicle communications system - *assign call signs to various vehicles.*
- (8) Arrange for HRP vehicle. Encode radios if possible.  
NOTE: *Consider using an armored vehicle where available.*
- (9) Arrange for 24-hour security of HRP vehicle.
- (10) Assign and brief all drivers of vehicles.
- (11) Select and develop emergency routes of travel and identify possible safe havens.
- (12) Attempt to estimate effect of adverse weather to HRP travel timetable.
- (13) Arrange for weather forecast for day of travel.

**e. Avoiding fixed patterns.** HRP protective personnel should take care that the HRP does not fall into a routine. Security personnel should develop a system that

## FOR OFFICIAL USE ONLY

ensures they and the HRP are *Systematically Unsystematic* in their everyday actions.  
Always:

<input type="checkbox"/> (1) Vary times of departure and arrival.
<input type="checkbox"/> (2) Vary the travel route.
<input type="checkbox"/> (3) Vary the vehicles used for transportation.
<input type="checkbox"/> (4) Park the vehicles in different locations each day.
<input type="checkbox"/> (5) Use different building entrances and exits.
<input type="checkbox"/> (6) Use different stairs and elevators.
<input type="checkbox"/> (7) Vary meal times and locations.
<input type="checkbox"/> (8) Limit the wearing of military uniforms in public areas.
<input type="checkbox"/> (9) Vary shift change times, guard post relief times, communications check-in times, and roving patrol routes.

### f. Meetings and/or social event security

<input type="checkbox"/> (1) Location.
<input type="checkbox"/> (2) Who will be attending?
<input type="checkbox"/> (3) Who will be providing security?
<input type="checkbox"/> (4) What security arrangements have been made?
<input type="checkbox"/> (5) Evacuation routes.
<input type="checkbox"/> (6) Location of nearest telephone.
<input type="checkbox"/> (7) Parking/driver arrangements.
<input type="checkbox"/> (8) Is press coverage anticipated?
<input type="checkbox"/> (9) Any gift exchange?

## 4. THE VISIT

<input type="checkbox"/> a. Ensure deviations to the scheduled plan are immediately reported to higher headquarters and explained. Ensure compensatory measures are taken as needed.
<input type="checkbox"/> b. Inspect facilities to be visited (event locations, restaurants, tourist areas, etc.) prior to the HRP arrival and ensure security arrangements are ready.
<input type="checkbox"/> c. Conduct a daily inspection of the HRP vehicle incorporating the following checks:
<input type="checkbox"/> (1) Slowly walk around the vehicle visually inspecting it and its surroundings for any sign of tampering or contact (dust and hand-print inspection).
<input type="checkbox"/> (2) Closely inspect vehicle for signs of entry.
<input type="checkbox"/> (3) Visually inspect the underside of the vehicle.
<input type="checkbox"/> (a) All frame members (inspect plugs in box frames).
<input type="checkbox"/> (b) Fuel tank (top, sides, and bottom - filler pipe).
<input type="checkbox"/> (c) Fender wells, suspension, steering , and drive shaft.
<input type="checkbox"/> (d) Muffler(s) and exhaust pipe.
<input type="checkbox"/> (e) Behind bumpers.

## FOR OFFICIAL USE ONLY

<input type="checkbox"/> (f) Tires (inspect the bottom, front, and rear part of the tire for pressure release firing devices).
<input type="checkbox"/> (4) Open the hood and visually inspect the engine compartment.
<input type="checkbox"/> (a) Air filter intact.
<input type="checkbox"/> (b) Fire wall is clear.
<input type="checkbox"/> (c) Other special areas as required.
<input type="checkbox"/> (5) Unlock the trunk and visually inspect the compartment.
<input type="checkbox"/> (a) Remove and inspect all security and safety containers.
<input type="checkbox"/> (b) Remove the mats and cosmetic panels.
<input type="checkbox"/> (c) Inspect back of rear passenger seat (rear axle hump), fuel tank and fender areas.
<input type="checkbox"/> (6) Open all vehicle doors and visually inspect the under-seat area (front and rear) to include floor carpets.
<input type="checkbox"/> (7) Visually inspect the underside of the dashboard area and the inside of the glove compartment.
<input type="checkbox"/> (8) Close all vehicle doors, hood, and trunk; lock all doors; check that all are operating properly.
<input type="checkbox"/> (9) Check for proper inflation of each vehicle tire with a quality tire gauge; inflate tires to exact pressure required (includes spare tire).
<input type="checkbox"/> (10) Check all fan belt conditions and tensions.
<input type="checkbox"/> (11) Check battery tie down system and battery terminals for tightness and corrosion.
<input type="checkbox"/> (12) Check all vehicle fluids: oil, power steering, power brakes, coolant, window washer, and battery acid level; fuel tank should be no less than one-half full.
<input type="checkbox"/> (13) Visually inspect ignition system wiring for tightness and condition.
<input type="checkbox"/> (14) Clean all vehicle windows and mirrors.
<input type="checkbox"/> (15) Check that all vehicle lights are operational; clean headlights, fog lights, and tail lights.
<input type="checkbox"/> (16) Start engine and check all vehicle gauges, indicator lights and operational equipment (power windows, electrical door locks, windshield wipers, horn, turn indicators, etc.).
<input type="checkbox"/> (17) Test all special purpose vehicle radios, alarms, signaling devices and special systems to ensure that they are operational.
<input type="checkbox"/> (18) Ensure air condition/heating systems are functional.

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**M-3-B-6  
FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### TAB C (NON-TACTICAL ARMORED VEHICLE PROGRAM) TO APPENDIX 3 (HIGH RISK PERSONNEL) TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPOD 01-01

#### REFERENCES: See Basic Order

**1. SITUATION.** Because of a combination of factors, non-tactical armored vehicle (NTAV) support may be required to enhance the protection of certain designated individuals.

**2. MISSION.** To set forth USEUCOM policy and guidance for the procurement, assignment and use of NTAV assets.

#### 3. EXECUTION

**a. Scheme of support.** This Tab applies to all Service component commands, direct reporting units (DRU), and any Joint Task Force/Combined Task Force (JTF/CTF) established and/or operating in the USEUCOM AOR.

##### b. Tasks and Responsibilities

###### (1) HQ USEUCOM

###### (a) ECSM

(1) Provides oversight of component management of the NTAV program.

(2) Has the authority to direct the transfer of NTAV assets between components when an immediate higher-priority need arises that cannot be met by the responsible component and all other means to obtain an armored vehicle, i.e., lease or borrow, have been considered.

(3) Reviews for approval all component requests:

(a) To procure or acquire by long-term lease fully armored vehicles (FAV).

(b) To place light armor on new vehicles or vehicles already in the inventory (Light Armored Vehicle, LAV).

(c) To transfer NTAV assets between countries for a period in excess of 30 days.

(4) Maintains an inventory control register of all NTAV within the USEUCOM AOR. This register will include as a minimum the information listed in Exhibit 1 to this TAB.

(b) ECJ2. Validates threat assessments accompanying requests for NTAV support.

###### (c) ECJ4

M-3-C-1

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

(1) Serves as HQ USEUCOM point of contact for the logistical management of the NTAV program for security assistance organizations.

(2) With the coordination of ECSM, manages the allocation of NTAV assets for security assistance organizations.

### **(2) Service component commanders and DRU chiefs/commanders**

(a) Submit requests to purchase or acquire by long-term lease FAV assets to HQ USEUCOM ECSM for further processing with the DoD proponent for the program. (This does not apply to the one-for-one replacement of FAV assets already in the inventory.)

(b) Ensure vehicles to be light armored have heavy duty equipment or components and an engine with sufficient horsepower to accommodate the added weight of light armoring materials.

(c) Ensure all transparent armor and armoring materials in the vehicle windows and in the body of a LAV are removed before turning in the vehicle for disposal. Certify such removal or destruction of armoring materials on the appropriate component Motor Vehicle Accountability/Disposal Record Reports.

(d) Immediately notify HQ USEUCOM/ECSM of any attack on a NTAV, or if a NTAV is lost or stolen.

(e) Maintain inventory control of all NTAV assets under their management control. As a minimum, the database will include the information in Exhibit 1 to this TAB.

(f) Determine distribution of all NTAV assets under their management control based on guidance provided in paragraph 4a, below. (Threat and vulnerability assessments mentioned in paragraph 4a will be conducted by respective security and intelligence elements supporting the activity.)

(g) Validate requirements for NTAV assets and update component distribution plans at least annually.

(h) In distributing NTAV assets, provide those high-risk DoD officials serving in NATO or other international billets the same consideration for support as all other high-risk DoD officials using the guidelines of DoDI 2010.1, Support of International Military Activities.

(i) Notify HQ USEUCOM/ECSM prior to relocating NTAV assets from one country to another. Inform ECSM by message when any NTAV is to be relocated within the same country for more than 30 days.

**M-3-C-2**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

(j) Fund support for NTAV assets within EUCOM to include fuel, maintenance and long/short term lease expenses. The component command will support additional assets that are required as a result of increased operational requirements.

### c. Coordinating instructions

(1) NTAV assets within the USEUCOM AOR provide protection to selected high-risk DoD officials, including those assigned to international positions, in performance of their duties and/or at other times on the basis of specific threat and vulnerability assessments that infer a clear and present danger from terrorism. Provide vehicles on an area support basis to have flexibility in the use of NTAV assets to protect all other high-risk DoD personnel who are potential terrorist targets. When possible, pool vehicles for rotation among authorized users to enhance security.

(2) DoD policy regarding the allocation of FAV assets to certain designated positions is contained in reference (l). Allocate all remaining NTAV assets as stated in paragraph 3c(1), above.

(3) Authorizations for the procurement or long-term lease of additional FAV assets shall be approved only on a case-by-case basis. Requests for such approvals should be sent to HQ USEUCOM ECSM for review prior to submission to the designated approving authority per reference (l).

(4) Approval shall be granted only in those circumstances in which the threat to DoD personnel clearly warrants an increased protection that cannot be provided by other means.

(5) Procurement of FAV assets is authorized on a one-for-one replacement basis for vehicles already in the inventory.

(6) Results of annual component command reviews and distribution plans will be forwarded to HQ USEUCOM ECSM. Classify reports as necessary to protection sensitive design data and/or system vulnerabilities.

(7) Each NTAV user will ensure that vehicle use is consistent with the statutory requirements for authorizing government transportation support in areas outside of CONUS.

(8) Vehicle modifications that reduce NTAV protective capabilities should not be made without the prior approval of HQ USEUCOM ECSM. When a NTAV is rendered inoperable for a period in excess of 30 days, notify HQ USEUCOM ECSM. This requirement is designed to improve the accuracy of NTAV accountability, and to identify early-on the loss of capability resulting from local modifications, e.g., removing windshields or anything else that makes the NTAV less effective.

**M-3-C-3**

**FOR OFFICIAL USE ONLY**

## **FOR OFFICIAL USE ONLY**

**(9)** Use of a NTAV is but one element in a comprehensive personal security program. To be effective, the vehicle driver must be qualified in antiterrorism evasive driving techniques.

**(10)** There are specialized defensive driver training courses available for high-risk personnel, their drivers, and security detail personnel. The courses are designed to teach driving techniques and methods of evading a terrorist attack. Requests for information on the location/cost of such training should be sent to the HQ USEUCOM ECSM.

**(11)** Smoking in NTAVs is prohibited. Smoke by-products damage the laminates used in the transparent armor.

### **EXHIBITS:**

1. Annual non-Tactical Armored Vehicle (NTAV) Reporting Format



## FOR OFFICIAL USE ONLY

### EXHIBIT 1 TO TAB C (NON-TACTICAL ARMORED VEHICLE PROGRAM) TO APPENDIX 3 (HIGH RISK PERSONNEL) TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPOD 01-01

#### ANNUAL NON-TACTICAL ARMORED VEHICLE (NTAV) REPORTING FORMAT

##### 1. Fully Armored Vehicle (FAV) Report:

- a. Make and year of vehicle.
- b. Date (fiscal year), place procured, and FAV cost.
- c. Location of FAV.
- d. Local organization (not component command) controlling the FAV use (state complete mailing/messages addresses and telephone numbers).
- e. Principal(s) protected by FAV (titles, names, and positions). If there are no designated principal(s), state the primary use of the vehicle, e.g., area support.
- f. Date of last threat and vulnerability assessment used to determine FAV deployment.
- g. General Comments:
  - (1) Identification of FAVs turned in or not in service, reasons for such action since the last NTAV report.
  - (2) Contemplated future FAV procurement/replacement and rationale.
  - (3) Lessons learned and recommendations to improve the FAV Program.
  - (4) List leased (short and/or long term) and "on loan" FAVs in this subparagraph along with the identity of the leasing company or the organization that was the source of the FAV.

##### 2. Light Armored Vehicle (LAV) Report:

- a. Make and year of vehicle.
- b. Date (fiscal year), place procured.
- c. Date Fiscal year) and place armored.
- d. Vehicle cost and LAV modification.

**M-3-C-1-1**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

**e.** Location of LAV.

**f.** Local organization (not Component Command) controlling the LAV use (state complete mailing/messages addresses and telephone numbers).

**g.** Principal(s) protected by LAV (titles, names, and positions). If there are no designated principal(s), state the primary use of the vehicle, e.g., area support.

**h.** Date of last threat and vulnerability assessment used to determine LAV deployment.

## FOR OFFICIAL USE ONLY

### TAB D (EVASIVE DRIVER TRAINING FOR HIGH-RISK PERSONNEL) TO APPENDIX 3 (HIGH RISK PERSONNEL) TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPORD 01-01

#### 1. BACKGROUND

a. Transportation security is a critical antiterrorism issue. Empirical data and statistical evidence clearly indicates this is one of, if not the most, vulnerable time periods for targeting and attack of high risk personnel by terrorists. Providing trained drivers is at least as important as other transportation security measures to include armored vehicles, protective service details and special authority to use government transportation for unofficial travel (home to work, etc.).

b. Armored vehicles are designed to provide additional protection and increase a driver's ability to escape from an attack site. Without specialized driver training, an armored vehicle loses much of its capability. Trained drivers, first and foremost, are aware of measures that reduce vulnerability. They also learn how to detect potential threats and finally how to use evasive driving procedures if necessary. MSgt Robert Judd survived a terrorist attack in a normal vehicle because he knew and applied evasive driving procedures. Mr. Leamon Hunt, Director General of the Multinational Force and Observers, was killed in an armored vehicle because his driver did not. A number of successful or "near miss" attacks may have been prevented, foiled or reacted to in a more appropriate fashion, if the driver had been properly trained and had applied these lessons and skills. The attack on General Frederick Kroesen is a classic example of the latter.

c. Procedures exist to authorize High-Risk Personnel (HRP) the use of government transportation for unofficial travel (home-to-work, etc.) if certain conditions are met. **Such unofficial use must also satisfy a number of IRS requirements to avoid significant tax liabilities.** For example, if a driver is provided, the valuation of such "chauffeur" services is "the amount that an individual would have to pay in an arm's-length transaction to obtain the same or comparable chauffeur services in the geographical area, including the time the chauffeur is on call as well as actual driving time" (Treasury Regulation 1.61-21(b)(5)(i)(A)). To exempt this value from taxable income the individual must meet certain requirements. "If an employer provides an employee with vehicle transportation and a bodyguard/chauffeur for a bona fide business-oriented security concern, and but for the bona fide business-oriented security concern the employee would not have had a bodyguard or a chauffeur, then the entire value of the services of the bodyguard/ chauffeur is excludable from gross income as a working condition fringe. For purposes of this section, a bodyguard/ chauffeur must be trained in evasive driving techniques. **An individual who performs services as a driver for an employee is not a bodyguard/chauffeur if the individual is not trained in evasive driving techniques.** Thus, no part of the value of services from such an individual is excludable from gross income under paragraph (m) (5), Treasury Regulation 1.32-5 (m)(5)).

M-3-D-1

FOR OFFICIAL USE ONLY

# FOR OFFICIAL USE ONLY

## 2. POLICY

a. The following personnel will successfully complete antiterrorist evasive driver training:

(1) Personnel who operate non-tactical armored vehicles for the purpose of transporting HRP.
(2) Personnel assigned to drive for individuals officially designated as HRP, see Annex M, Appendix 3 of this OPORD.
(3) Service members and DoD Civilians who have been officially designated as an HRP and frequently operate government vehicles.
(4) Personnel assigned to drive for individuals who are authorized the use of government transportation for unofficial travel due to security reasons.
(5) Personnel who are authorized the use of government transportation for unofficial travel due to security reasons and drive the government vehicle themselves.

b. Antiterrorism evasive driver training should be considered for Service members and DoD Civilians who are permanently stationed in an area where the Terrorism Threat Level is High and frequently operate government vehicles off of a U.S. facility.

c. Antiterrorist evasive driver training courses must be approved by DoD, an individual Service, Defense Agency (e.g., DIA, DTRA), or other U.S. Government Department (e.g., Justice, FBI, State Department). The evasive driver training can be separate or part of a related course (e.g., Protective Service Agent Training).

d. Proficiency in evasive driving requires periodic training since these unique and generally unused skills are perishable. All personnel required to attend an evasive driving course should receive refresher training and be provided the opportunity to practice these skills at least annually. Maximize the use of in-country training opportunities (mobile training teams, Defense agencies, U.S. Embassy Regional Security Officers, etc.).

**3. DRIVER QUALIFICATIONS.** Selecting a driver is at the discretion of the individual charged with hiring the driver using guidance provided by his/her Service or Agency. The following information should assist those personnel who may not be familiar with desirable characteristics for a specialized driver, particularly when screening local national hires.

a. An interview can help to determine the driver's ability to speak and understand English. An interview can also provide insight into how the candidate feels about driving under hazardous conditions, about damaging the vehicle in attempting to avoid an attack, and the driver's knowledge concerning his duties. Having the candidate take a road test can provide invaluable information. Characteristics to look for include the driver's general comfort level with operating the vehicle, coordination, style of driving (overly aggressive or timid drivers are generally unsuitable), is the candidate observant or does he/she tend to "daydream," and any previously unidentified traits.

**FOR OFFICIAL USE ONLY**

**b. Physical and Mental.**

(1) Height proportioned to weight.
(2) Physically fit.
(3) Coordination (good dexterity, agile).
(4) No disabling features or significant health problems.
(5) Excellent hearing and vision.
(6) No history of mental problems.
(7) Mature and possessing common sense.
(8) Capable of learning.

**c. Verbal Communication.** Speaks English. Has no hard accent that may make spoken English unintelligible. No communication problem that would make emergency communications difficult.

(1) Driving Ability and skills.
(2) Extensive driving experience.
(3) Excellent driving record.
(4) Experience in driving on snow, mud, or ice (where applicable).
(5) Not intimidated by traffic.
(6) Knowledge of local laws.
(7) Observant.

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**M-3-D-4**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### APPENDIX 4 (FIREARMS FOR PERSONAL PROTECTION) TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPOD 01-01

**REFERENCES:** DoD Directive 5210.56, 25 Feb 92 with Change 1, 10 Nov 97

**1. GENERAL.** This Appendix provides policy and guidance for personnel for whom USCINCEUR is responsible to authorize the carrying of firearms for personnel protection.

**a.** This Appendix does not apply to personnel performing operational or training missions, personnel who are in a combat zone or hostile fire area, or personnel who carry a weapon as a normal course of their duties such as law enforcement or security personnel.

**b.** This Appendix does not supersede Service component command authority vested by their various Services to authorize the use of firearms for personal protection.

**2. POLICY.** It is the DoD policy to limit and control the carrying of firearms by DoD personnel. An authorization to carry firearms may be issued only when there is a reasonable expectation that life or property will be jeopardized if firearms are not carried. Evaluation of the necessity to carry a firearm shall be made considering this expectation and the possible consequences of accidental or indiscriminate use of firearms. Authorization will be for a period not to exceed 1 year. Users may request an extension of the authorization. A continual evaluation of the threat will be conducted to determine the need to extend or terminate the authorization to carry firearms.

### **3. PROCEDURES**

**a.** Military personnel may be authorized to carry government owned firearms for personal protection in the USEUCOM AOR only after intelligence analysis identifies a credible threat against the U.S. personnel in the area. Firearms will not be issued indiscriminately for this purpose. For all personnel other than those assigned/attached and under the authority of a Service component commander, USCINCEUR or his designated representatives (the Deputy USCINCEUR or HQ USEUCOM Chief of Staff), are the only individuals who may authorize personnel, on a case-by-case basis, to carry firearms for personal protection. Authorization is only applicable for the geographic location approved by USCINCEUR or his designated representative.

**b.** Any person issued a weapon for personal protection must receive, in advance, qualification and certification training on the weapon to be carried. In addition, prior to submitting the request, commanders must screen the individual's medical and personnel records to ensure reliability and suitability for carrying a firearm. Commanders must submit a written and signed document with the request indicating these records have been reviewed. At geographically separated units, commanders can request these records from the component personnel section at HQ USEUCOM. The records may either be faxed or sent registered mail, depending on the component.

**M-4-1**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

Commanders retain all supporting documentation on file at their unit or activity for at least one year after individual is no longer authorized to carry a firearm for personal protection.

**c.** Prior to authorization mandatory training must include:

**(1)** Attendance at a course designed to train personnel on how to draw and fire a concealed weapon, e.g., the High-Risk Personnel (HRP) course at Quantico, VA. Resident instruction may be waived, but the Program of Instruction (POI) should be similar to HRP course. Individuals must be familiar with the use of actual equipment (holster rig) in which the firearm will be carried.

**(2)** A thorough briefing on individual responsibilities.

**(3)** Use of deadly force and Rules of Engagement (ROE) training.

**(4)** Instructions on safety functions, capabilities and limitations of the weapon to be carried.

**(5)** As a minimum, proficiency testing must include annual qualification training.

**(6)** In addition, the unit or activity commander must ensure that each individual seeking authorization complete DD Form 2760, Qualification to Possess Firearms or Ammunition. This form certifies whether or not the individual in question has been convicted of a misdemeanor crime of domestic violence. Do not request authority to carry firearms for those personnel who have been convicted of a misdemeanor crime of domestic violence.

**d.** USEUCOM activities assigned to U.S. diplomatic missions must include the following in their request:

**(1)** Guidelines for the carrying and discharge of firearms that take into account U.S. government regulations, international agreements, and host country laws. Request must include applicable host nation laws and U.S. agreements and whether or not a host nation permit is required.

**(2)** Statement indicating concurrence of the COM.

**e.** Forward all requests to HQ USEUCOM ECSM for processing. ECSM will forward request to the approving authority for approval. ECJA will review the request for legal sufficiency.

**f.** If these personnel carry firearms in uniform, the sidearm will be visible. When the threat environment or operational need dictates the carrying of a concealed weapon,



## FOR OFFICIAL USE ONLY

individuals will comply with their parent Service or agency requirements concerning documentation.

**g.** Per DoDD 5210.56, personnel are authorized to carry only government-owned and issued weapons and ammunition.

**h.** Per DoDD 5210.56, safety lock devices and instructions for their proper use shall be provided with all firearms issued to such personnel who have been authorized to retain firearms at their residence or non-government locations.

**i.** Report any discharges resulting in personal injuries or property damage using OPREP-3.

### ACKNOWLEDGE:

**JOSEPH W. RALSTON**  
General, USAF

### TAB:

A. Sample Request for Request for Authority to Bear Firearms for Personal Protection

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**M-4-4**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### TAB A TO APPENDIX 4 (FIREARMS FOR PERSONAL PROTECTION) TO ANNEX M PHYSICAL SECURITY) TO USCINCEUR AT/FP OPORD 01-01

#### SAMPLE REQUEST FOR AUTHORITY TO BEAR FIREARMS FOR PERSONAL PROTECTION

Below is a sample request for Authority to Bear Firearms for Personal Protection. In lieu of the information in paragraph 4, below, units/activities may submit a completed DA Form 7281-R and DD Form 2760.

#### UNIT LETTERHEAD

Date

MEMORANDUM FOR: USCINCEUR, Attn: ECSM, Unit 30400, Box 1000  
APO AE 09128

SUBJECT: Request for Authority to Bear Firearms for Personal Protection

1. Request authorization for the following individual to bear a U.S. Government firearm for personal protection:

- a. Rank
- b. Name
- c. SSN
- d. Branch of Service
- e. Unit of Assignment
- f. Duty Location (City / Country)
- g. Weapon type: (Make, Model, caliber)
- h. Serial Number (primary)
- i. Serial number (alternate)

2. The following information supports this request:

a. (State the reason for this request, the desired duration of the authorization, and whether the weapon is to be carried in a concealed manner. Include information concerning the credible threat and/or heightened Force Protection Condition. In many instances this information will be sensitive or classified. A classified threat assessment may be provided as an enclosure if appropriate.)

b. A security assessment was conducted during (month/year). This assessment evaluated the threat to \_\_\_\_\_ from acts of terrorism and recommended security measures that are necessary to provide him/her with protection commensurate with that threat. One of the recommendations was that \_\_\_\_\_ be authorized to bear a firearm for personal protection.

**M-4-A-1**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

c. State whether or not a protective services detail (military or host nation) is provided. If a protective services detail is not provided, comment on the reasons why.

d. Additional personal security measures in effect include: (e.g. varying of travel routes, residence security measures, office security measures, use of body armor, use of driver trained in evasive driving, use of an armored vehicle, use of a government vehicle for home to work and other unofficial travel, specialized security training, etc.)

3. (Rank Name) has qualified with this firearm within the last twelve months. A copy of the qualification record is enclosed. It is understood that (Rank Name) must maintain a current qualification (at least every twelve months) while this authorization is in effect. In addition, this person attended a formal weapons training course that included drawing and firing a concealed weapon at (give course name and location) to prepare for this authorization. Request waiver of requirement to attend formal training, this training will be provided on location by a qualified instructor. Additionally, (Rank Name) has been briefed on individual responsibilities; the use of deadly force; and instructions on the safety functions, capabilities, and limitations of the weapon(s) to be carried.

4. The following screening procedures have been accomplished:

- a. Personal Interview
- b. Personnel Records Review
- c. Medical Records Review
- d. Military Law Enforcement/Security Office Review
- e. Local Civilian Police Records Check
- f. Individual has completed DD Form 2760 (certifying that he/she has not been convicted of a misdemeanor crime of domestic violence).

5. After thorough review of all information provided, I find this individual suitable to bear a firearm for personal protection. All information and qualification records pertaining to this individual will be maintained on file with this command for at least one year after the individual in question departs on PCS orders. POC for this request is (include rank, name, duty position, DSN Phone, commercial phone, fax number, and mailing address).

SIGNATURE BLOCK

**M-4-A-2**  
**FOR OFFICIAL USE ONLY**

# FOR OFFICIAL USE ONLY

## APPENDIX 5 (AT/FP TRAINING) TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPOD 01-01

### REFERENCES: See Basic Order

**1. SITUATION.** Developing a high state of situational awareness and understanding of personal AT/FP responsibilities is essential to ensure the safety and security of DoD personnel and facilities. An effective AT/FP training program for personnel and family members at all echelons contributes to achieving this objective.

**2. MISSION.** To establish policy and procedures for a comprehensive AT/FP training program throughout USEUCOM.

### 3. EXECUTION

**a. Scheme of support.** This appendix outlines opportunities for AT/FP related training and responsibilities related to AT/FP training. Table M-5-1, below, outlines the four levels of AT/FP training requirements.

#### **b. Tasks and Responsibilities**

##### **(1) HQ USEUCOM**

###### **(a) ECSM**

**(1)** Act as the HQ USEUCOM Office of Primary Responsibility (OPR) for AT/FP training policies, procedures, and directives.

**(2)** Review requests for new programs and revisions to existing programs.

**(3)** Ensure the validity of training objectives and ensures the directing agency addresses all requirements specified in this Appendix.

**(4)** Provide assistance and information to improve the quality and effectiveness of the AT/FP training program.

**(5)** Monitor the impact of AT/FP training on mission accomplishment and personnel, as reported by the component commands and through command inspection and visitation programs.

**(6)** Coordinate specialized training for senior leaders.

**(7)** Provide input to ECJ3 for AT/FP training requirements associated with operations and the Joint Mission Essential Task List (JMETL).

**(b) ECJ1.** In coordination with Component Command personnel directorates, ensure all individual orders for PCS or TDY indicate that the individual is required to receive Level I AT/FP training prior to deployment to this AOR.

**(c) ECJ2.** Assist ECSM in developing policies related to individual and unit intelligence training.

**M-5-1**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

**(d) ECJ3.** Develop overall training requirements for operations and exercises. Act as OPR for the JMETL. In coordination with ECSM, develops AT/FP JMETL tasks.

**(e) ECIG.** In coordination with ECSM, conduct USEUCOM-wide inspections to determine the effectiveness of AT/FP training management and integration of training assets with doctrine and tactical development, resource allocation, and training execution.

**(f) ECPA.** Provide public affairs guidance to in-theater antiterrorist training.

**(2) HQ USAREUR.** Act as the Command Executive Agent for the in-theater Antiterrorism Evasive Driving (ATED) Course. This responsibility includes overall theater management and the funding of HQ USEUCOM personnel.

**(3) All Theater Clearance Granting Authorities.** Deny theater clearance to any DoD element or individual deploying to this AOR, unless they certify that all personnel deploying have received required Level I AT/FP training.

### **(4) All DoD Commands/Services/Agencies/Activities.**

**(a)** Ensure all assigned/attached/OPCON/TACON personnel receive individual antiterrorism awareness training prior to deploying or traveling to the USEUCOM AOR. In case of a no-notice deployment, units must give or coordinate for Level I training at the earliest opportunity after deploying to the USEUCOM AOR.

**(b)** Ensure this training includes:

- (1)** Individual security awareness and individual force protection.
- (2)** AOR or country-specific information on the terrorist threat.
- (3)** A briefing on the current country-specific Force Protection Condition

in effect.

**(4)** Instruction on recognizing and reporting improvised explosive devices (IED); e.g., in packages, baggage, motor vehicles.

**(5)** Mine Awareness Training, as appropriate.

**(6)** Personnel designated as being at high risk to terrorist attack and personnel assigned to high risk billets must receive advanced AT/FP training. Give this training to family members, as appropriate.

**(7)** DoD personnel and family members assigned to locations where the Terrorism Threat Level is promulgated above "MODERATE" must receive guidance on appropriate conduct in the event they are taken hostage or kidnapped at least annually.

**(8)** Supplement training with use of deadly force/rules of engagement (scenario based) training for all individuals required to perform security and law enforcement related duties. Ensure this training is accomplished within 72 hours after arrival in the AOR and prior to the performance of such duties. This training will be

**M-5-2**

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

approved by the servicing Judge Advocate General and senior security/military police officer.

**NOTE:** DoD personnel being assigned to positions under the security responsibility of the COM should receive required AT/FP training prior to reporting to their duty assignments. If this is not accomplished, the USDR should report such cases to HQ USEUCOM ECSM and DIA DAC-2D. Additionally, the Amembassy Regional Security Officer (RSO) will normally conduct newcomer briefings for those personnel under the security responsibility of the COM on a periodic basis, which will include personal protection information. DoD personnel and their family members are encouraged to attend these briefings; however, if these briefings do not meet the requirements specified in DoDI 2000.16, DoD AT Officers (ATO) remain responsible for ensuring proper/timely briefings are conducted.

(c) Require assigned personnel to review the unit/activity's antiterrorism plan/procedures as part of their antiterrorism briefing.

(d) Give refresher training every 12 months, as a minimum. A trained Level II ATO normally will provide this training. Exceptions may be granted for remote locations, where a trained officer is not available. As a minimum, refresher training should consist of the following topics:

- (1) Viewing Service-selected or DoD/Joint Staff personal awareness video.
- (2) Introduction to Terrorism.
- (3) Individual Protective Measures.
- (4) Detecting Surveillance.
- (5) Hostage Survival.

(e) Encourage accompanying family members (14 years or older) to attend newcomers and recurring briefings. Minors attending will be at the discretion of the parents.

(f) Document all briefings required by this Appendix. Retain related briefing records for review during higher headquarters AT/FP program reviews. Retain and file briefing records for one year on units/individuals affected by this Appendix.

(g) Brief personnel traveling TDY/TAD on the local threat and actions available to reduce the possibility of becoming the victim of a terrorist or criminal attack.

### c. Coordinating instructions

(1) To assist in developing plans, in preparing briefings, and as a reference for DoD policy and procedures, AT/FP offices should maintain (or, via the SIPRNET, have access to) a copy of DoD Handbook 0-2000.12-H. This publication is available at [http://www2.eucom.smil.mil/hq/ecsm/ecsm\\_home.htm](http://www2.eucom.smil.mil/hq/ecsm/ecsm_home.htm).

## **FOR OFFICIAL USE ONLY**

**(2)** Tenant organizations should coordinate with the installation/activity commander for Level I AT/FP training and/or country-specific threat updates for their personnel, as required.

**(3)** Additional information to assist in the preparation of antiterrorism briefings can be found on the HQ USEUCOM Force Protection Homepages on the SIPRNet and NIPRNet.

**(4)** Available training. Each Service is constantly updating its course selection. Check with HQ USEUCOM ECSM or the appropriate Service component command for an updated list of courses and course requirements.



**FOR OFFICIAL USE ONLY**

**Table M-5-1. Pre-deployment and Career Development AT/FP Training Requirements**

{PRIVATE}Level of Training	Target Audience	Minimum Training Standard
<p>Level I AT Awareness Training provided annually to:</p> <p>(1) All OCONUS-based DoD personnel</p> <p>(2) All Active uniformed CONUS-based members of the CINCS and Services</p> <p>(3) All CONUS-based DoD personnel eligible for official OCONUS travel on government orders</p> <p>(4) All CONUS-based DoD personnel regardless of duty status if the CONUS Terrorism Threat Level is promulgated above "MODERATE".</p> <p>**Graduates will have requisite knowledge to remain vigilant 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.</p>	<ul style="list-style-type: none"> <li>• DoD personnel Accessions during initial Training.</li> <li>• Military, Department of Defense Civilians, their family members 14 years old and greater (when family members are deploying or traveling on government orders), and DoD-employed Contractors.</li> </ul>	<p>Component-provided instruction; incorporates Component-standardized POI consisting of the following minimum topics:</p> <ol style="list-style-type: none"> <li>1. Viewing the Service-selected personal awareness video provided under the instruction of a qualified Level I AT Awareness instructor and/or DoD-sponsored, and Component-certified, computer-based and/or distance learning (DoD personnel accessions must receive initial training under instruction of a qualified Level I AT Awareness Instructor).</li> <li>2. Instruction on the following:               <ul style="list-style-type: none"> <li>• <i>Introduction to Terrorism</i></li> <li>• <i>Terrorist Operations</i></li> <li>• <i>Individual Protective Measures</i></li> <li>• <i>Terrorist Surveillance Techniques</i></li> <li>• <i>Improvised Explosive Device (IED) Attacks</i></li> <li>• <i>Kidnapping &amp; Hostage Survival</i></li> <li>• <i>Explanation of Terrorism Threat Levels and Force Protection Condition System</i></li> </ul> </li> <li>3. Issuance of JS Guide 5260 "Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism" and "Antiterrorism Individual Protective Measures" folding card. (Local reproduction of both is authorized).</li> <li>4. Receipt of AOR updates three months prior to travel to include current threat brief and AOR specific requirements as provided by the receiving geographic CINC.</li> </ol>
{PRIVATE}Level of Training	Target Audience	Minimum Training Standard
Level II	Officers/ NCOs/	Component-provided instruction (resident

**FOR OFFICIAL USE ONLY**

<p>AT Officer (ATO) Training</p> <p>** Graduates shall have requisite knowledge and materials to manage a comprehensive AT Program and advise the commander in all AT areas.</p>	<p>civilian staff officers, who are tracked and command-designated to serve as the AT advisor to the Commander and provide Level I Instruction in coded billets.</p>	<p>or MTT); incorporates Component-standardized POI consisting of the following minimum topics:</p> <ul style="list-style-type: none"> <li>• Understanding AT Roles and Responsibilities             <ul style="list-style-type: none"> <li>- Understand Policy &amp; Standards</li> <li>- Access Reference Sources</li> </ul> </li> <li>• Organize for AT             <ul style="list-style-type: none"> <li>- Command/Staff Relationships</li> <li>- FP Working Groups</li> </ul> </li> <li>• Assess Vulnerabilities             <ul style="list-style-type: none"> <li>- Baseline Unit FP Posture</li> <li>- Conduct Assessment</li> </ul> </li> <li>• Assess Threat             <ul style="list-style-type: none"> <li>- Intel / CI Integration</li> <li>- Information OPS</li> </ul> </li> <li>• Create and Execute AT Programs             <ul style="list-style-type: none"> <li>- Use of Terrorism Threat Level / Force Protection Conditions</li> <li>- Unit/Installation Protective Measures</li> <li>- Mitigating Vulnerabilities</li> </ul> </li> <li>• Prepare AT Plans             <ul style="list-style-type: none"> <li>- Templates &amp; Planning Tools</li> <li>- How to Develop &amp; Write Plans</li> <li>- WMD Considerations</li> <li>- Use of RAM to protect the Installation</li> </ul> </li> <li>• AT Resource Management             <ul style="list-style-type: none"> <li>- Requirements Generation &amp; Prioritization</li> <li>- CbT RIF</li> </ul> </li> <li>• Conduct AT Training             <ul style="list-style-type: none"> <li>- Exercise Unit AT Plans</li> <li>- Obtain AOR-specific updates</li> <li>- Oversee AT Level I Training</li> </ul> </li> </ul> <p>2. Review of DoD Directive 2000.12, Instruction 2000.16, Order 2000.12-H and other applicable Department of Defense/Service/Agency publications.</p> <p>3. Methods available for obtaining AOR-</p>
--	--	--

**M-5-6**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

		<p>specific updates for deployment/travel areas.</p> <p>4. Component-directed modules on other aspects of AT such as physical security requirements, technology updates, etc.</p>
<b>{PRIVATE}Level of Training</b>	<b>Target Audience</b>	<b>Minimum Training Standard</b>
<p>Level III Pre-Command AT Training</p> <p>**Graduates shall have requisite knowledge and materials to supervise a comprehensive AT Program and manage AT issues.</p>	<p>O-5/O-6 Commanders</p>	<p>Component-provided instruction during pre-command pipelines; incorporates Component-standardized POI consisting of the following minimum topics:</p> <ol style="list-style-type: none"> <li>1. Viewing the SECDEF/CJCS Video</li> <li>2. Directive/reference review <ul style="list-style-type: none"> <li>• Understanding AT Responsibilities <ul style="list-style-type: none"> <li>- Understanding Policy</li> <li>- Assessments</li> <li>- Off-Installation Housing</li> </ul> </li> <li>• Ensuring Preparation of AT Plans <ul style="list-style-type: none"> <li>- Baseline FP Posture</li> <li>- Mitigating WMD Attack</li> <li>- MOU's/MOA's</li> </ul> </li> <li>• Ensuring Conduct of AT Planning <ul style="list-style-type: none"> <li>-AT Plans &amp; Training</li> <li>-Level I Training</li> </ul> </li> <li>• Organizing for AT</li> <li>• Understand the Local Threat Picture <ul style="list-style-type: none"> <li>- Fusion of Intelligence</li> </ul> </li> <li>• Building a Sustainable AT Program <ul style="list-style-type: none"> <li>- Terrorism Threat Levels</li> </ul> </li> <li>• Executing Resource Responsibilities <ul style="list-style-type: none"> <li>- AT Resource Programs</li> <li>- Construction Standards</li> </ul> </li> <li>• Understanding Use of Force and ROE</li> </ul> </li> <li>3. Review of DoD Directive 2000.12, Instruction 2000.12-H, Order 2000.16, and other applicable Department of Defense/Service/Agency publications.</li> <li>4. Issuance of Commander's Handbook (Joint Pub 5260).</li> </ol>
<b>{PRIVATE}Level of Training</b>	<b>Target Audience</b>	<b>Minimum Training Standard</b>

**M-5-7**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

<p>Level IV AT Executive Seminar **Graduates shall have requisite knowledge and materials to provide oversight to AT Programs and Policies.</p>	<p>Officers in the grade of O6-O8 and Department of Defense civilians in equivalent grades selected by Services/CINCs/ Department of Defense Agencies who are responsible for AT programs or involved in AT policy, planning and execution.</p>	<p>CJCS Executive-level seminar hosted by J-34. Provides pertinent current updates, briefings, and panel discussion topics. Seminar includes 3 tabletop AT wargames aimed at facilitating interaction and discussion among seminar participants.</p>
---	---	--

**ACKNOWLEDGE:**

**JOSEPH W. RALSTON  
General, USAF**

## FOR OFFICIAL USE ONLY

### APPENDIX 6 (PROCEDURES FOR SCREENING AND HANDLING MAIL) TO ANNEX M (PHYSICAL SECURITY) TO USCINCEUR AT/FP OPOD 01-01

#### REFERENCES: See Basic Order

**1. PURPOSE.** When used in this appendix, the term “mail” applies to all mail, packages, and parcel deliveries, both inter-Theater and intra-Theater, to include APOs, international mail, local/host nation postal services, and commercial delivery services such as UPS, FEDEX, DHL, etc. The intent of the appendix is to assist in developing procedures and employing detection capabilities to prevent the introduction of an explosive device or other harmful material by means of the mail systems into US facilities or other locations where US personnel or employees are located. Use of this tactic to date has been very limited, but aggressors could resort to this tactic at any time. As we continue to harden our facilities and implement effective Force Protection Condition AT/FP measures to defeat other types of threats, attempts may be made to use the mail systems for hostile purposes. We must develop and exercise plans and capabilities to increase our defenses against attempted attacks through the mail systems. These plans, exercises, and capabilities will serve as deterrents, will increase our ability to defend ourselves should such attacks be identified as a threat, and will increase our chances of thwarting an unpredicted attack.

**2. CONCEPT.** Prior to implementing this strategy or elements thereof, review your existing mail reception and delivery systems. Also review existing assessment reports and/or conduct a supplemental vulnerability assessment/risk assessment of these operations, to determine potential vulnerabilities associated with mail delivery. Use these assessments to determine the most vulnerable points within the process and develop potential means of reducing these vulnerabilities. The example measures/actions detailed below are a good starting point to correct potential vulnerabilities. All procedures and recommended action must be coordinated with the local AT/FP program manager and the local AT/FP working group members. Do not attempt to develop these procedures without consulting mail organizations, military police/security forces, explosive ordnance disposal (EOD) unit, fire departments, engineers, and your medical support element. All activities that receive mail should be included in this coordination to ensure current or proposed procedures are comprehensive and functionally sound. Upon final approval, these procedures must become part of the basic installation security plan.

**3. MAIL SCREENING MINIMUM TRAINING AND STANDARD OPERATING PROCEDURES DEVELOPMENT.** Mail screening procedures have proven very effective. A major part of such screening is visual and physical recognition. Although some of the indicators or warning signs listed below seem obvious, in a day-to-day routine, they can be easily overlooked. Even those installations with the best screening technologies need to train their mail handlers to use these basic-screening techniques. The first step in effectively screening mail is to ensure all mail is routed through at least one person trained to screen postal material for signs it might contain an explosive

M-6-1

FOR OFFICIAL USE ONLY

## FOR OFFICIAL USE ONLY

device. Ideally, all mail would be routed through a central point for screening and distribution. Should such an arrangement prove impractical, personnel at all receiving points (APO, front offices, hotel desk clerks, etc.) should be trained in identifying suspect mail. The following list of recognition features for suspect mail should be used by personnel handling, processing, and delivering mail at all levels. Special emphasis should be given to training professional postal personnel and to staffs of identified "high risk personnel" (HRP).

### INDICATORS OF SUSPECT POSTAL MATERIAL

<input type="checkbox"/> Letters feel rigid, appear uneven or lopsided, or are bulkier than normal
<input type="checkbox"/> Oil stains are present on the wrapper
<input type="checkbox"/> Excessive amounts of postage are used
<input type="checkbox"/> Sender is unknown or no return address is given
<input type="checkbox"/> Name and title of addressee are not accurate
<input type="checkbox"/> The address is prepared to ensure anonymity of the sender (e.g., homemade labels, cut-and-paste lettering)
<input type="checkbox"/> The addressee does not normally receive personal mail at the office
<input type="checkbox"/> Handwriting of sender appears distorted or indicates a foreign style not normally encountered
<input type="checkbox"/> Weight: The letter or package seems heavy for its size. Letters will normally weigh up to 1 ounce. Effective postal bombs will weigh more than 2 ounces and require more postage. They may be unusually thick, i.e., 3/16 inch or more.
<input type="checkbox"/> Weight of the package is uneven.
<input type="checkbox"/> Package has an irregular shape, soft spots, or bulges.
<input type="checkbox"/> Cancellation or postmark location is different from the return address location.
<input type="checkbox"/> Protruding wires, tinfoil, strings, or components. (Some devices have come apart in the mail)
<input type="checkbox"/> Mailing appears to have been disassembled or re-glued
<input type="checkbox"/> Several combinations of tape are used to secure the parcel.
<input type="checkbox"/> Wrapping shows evidence of previous use or suspicious traces of glue, mailing labels, return addresses, or tape.
<input type="checkbox"/> The package emits a peculiar smell or suspicious odors (May smell like almonds or shoe polish)
<input type="checkbox"/> Contents of the parcel make a sloshing sound.
<input type="checkbox"/> Package makes a buzzing or ticking noise (This is unusual for a mail type device, but could be present for an explosive device that is delivered by a "local delivery service.")
<input type="checkbox"/> Loose components rattle around
<input type="checkbox"/> A small hole in the envelope or package wrapping (a provision for an arming/safety wire)
<input type="checkbox"/> Restrictive markings, e.g., "confidential," "personal."
<input type="checkbox"/> Unprofessionally wrapped parcel is endorsed "Fragile- Handle with Care" or "Do not Delay"
<input type="checkbox"/> Misspellings of common words
<input type="checkbox"/> Visual distractions such as pornography or currency
<input type="checkbox"/> Pressure or resistance is noted when removing the contents

#### 4. SUSPECT PACKAGE HANDLING PROCEDURES.

**M-6-2**  
**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

a. Develop procedures using United States Postal Service (USPS) guidelines, in coordination with EOD and MP/SF, to respond to suspect mail. Some basic guidelines follow.

<input type="checkbox"/> <b>DO NOT OPEN THE ARTICLE</b>
<input type="checkbox"/> Isolate the package and secure the immediate area. Contact the MP/SF, who will establish a cordon and contact the responsible EOD element.
<input type="checkbox"/> <b>DO NOT</b> put the article in water or a confined space such as a desk drawer, safe, or filing cabinet. EOD will need ready access to the suspect package—pre coordinate suspicious package SOPs with your responsible EOD and MP/SF.
<input type="checkbox"/> If possible, open windows and doors in the immediate area to assist in venting pressure should an explosion occur. Evacuate adjacent rooms (upper, lower and sides) and adjacent outside areas.
<input type="checkbox"/> Once contact is made with the emergency response element, make sure you have someone who is familiar with the device (location and other specifics) immediately available to meet the first responders to describe the item and to expedite access.

b. Establishing a Quick Reaction Checklist (QRC) for dealing with suspect packages and posting it where mail clerks have ready access to it may be helpful in ensuring all required steps are taken when reacting to suspicious mail.

### 5. MORE ADVANCED SCREENING TECHNIQUES AND EQUIPMENT.

a. Before expending limited resources to procure a scanning system, evaluate the threat, determine your requirements, employ low cost solutions, and consult technical references and official sources of assistance. Determine how and where you plan to use a scanning device. Conducting an assessment of the mail/package delivery process on your installation/facility is an ideal way to determine your requirements. Once you understand your local process, then determine what procedural measures could be changed to streamline and centralize the process. Ideally, all mail should be delivered to one central mailroom or other delivery point for screening and subsequent distribution. If you decide to establish a mail/delivery screening area, consider locating this facility to take into account the addition of other security screening devices (such as explosives detection equipment). Also, since an explosive or other dangerous device could be delivered to such a facility, place these facilities away from any sensitive equipment or facilities that hold large numbers of personnel.

b. Technological experts have validated that large volume mail screening is costly and in many cases requires significant additional manpower and equipment. Short-term and lower cost solutions include use of available military Explosive Detector Dog Teams (EDDTs) and on-hand x-ray machines. While EDDTs are recognized as being highly effective, they also have limitations, and more importantly are already over-tasked. Any use of this high demand resource will take direct coordination with your local security forces/military police. If available, these teams can quickly and effectively

## FOR OFFICIAL USE ONLY

screen packages and delivery trucks. Include the use of EDDTs in your plans and exercises as a Random Antiterrorism Measure (RAM). To the extent possible, exercise coordination for and use of these assets on a regular basis, quarterly if possible. Additionally, use available technology. Although the x-ray screening devices currently in use have many limitations, they do provide additional capability over simple visual examination and increase the potential for identifying an explosive device.

c. Long-term solutions will require pre-screening of mail in an effort to cut down on the quantity of mail that will require detailed technological examination (back-scatter x-ray, metal detection, etc.). Some potential pre-screening techniques follow:

Separate Official, Personal and Foreign mail (official and foreign mail is probably a more likely terrorist target)
---

Examine High Profile/High Risk Personnel's mail/packages with available technology (for example, commanders, designated high risk personnel (HRP), and personnel in the news)
---

Use the suspect mail screening guide in paragraph 3 above—use technology to screen those that fit the suspect criteria (for example, only screen packages or letters weighing more than 1 ounce. Effective postal bombs will weigh more than 2 ounces and require more postage.)
--

d. For installations that are examining procurement of Explosive Detection Equipment (EDE), the Department of Defense has established a home page detailing a variety of resources and materials on EDE and the EDE program (<http://www.explosivedetection.nfesc.navy.mil>). This site also includes a technical information library that has a summary of current explosive detection technology. In addition, the site contains the Catalog of Explosive Detection Equipment and other EDE program products. The site also provides a three-page document, "Procurement Considerations" and provides a detailed list of questions that you can present to EDE vendors prior to ordering. Finally, command science advisors and component and EUCOM AT/FP offices may be of assistance in defining your requirements and identifying appropriate EDE to fulfill your needs.

**6. SUMMARY.** To date, use of postal and package delivery systems to introduce a bomb or harmful material onto DoD facilities has been very limited, but aggressors could resort to this tactic at any time. Prudent policies and procedures must be developed and implemented to prevent such attacks should they be attempted without warning and to prepare for them should intelligence sources provide warnings of such attacks. Initial steps should include implementing low cost measures such as manual screening of mail, using on-hand technology such as x-ray machines, and periodically employing EDDTs. To increase our capability to screen more mail on a more regular basis, we should establish screening procedures, identify technological solutions, and obtain funding for them through the normal budgeting process. Emphasis should be placed on making everyone from professional postal personnel to individual service

M-6-4

FOR OFFICIAL USE ONLY



**FOR OFFICIAL USE ONLY**

members and civilian employees aware of the characteristics of suspect packages and procedures for handling suspect packages.

**ACKNOWLEDGE**

**JOSEPH W. RALSTON**  
General, USAF

**M-6-5**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**M-6-6  
FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

### ANNEX Q (FORCE HEALTH PROTECTION REQUIREMENTS) TO USCINCEUR AT/FP OPORD 01-01

#### REFERENCES: See Basic Order

- 1. PURPOSE.** To provide guidance for the execution and oversight of USCINCEUR's AT/FP program as it applies to Force Health Protection.
- 2. APPLICABILITY.** This Annex applies to all units operating in the USEUCOM AOR and subordinate USEUCOM joint activities to include USDRs, DRUs, and JTF/CTFs.
- 3. BACKGROUND.** Soldiers, Sailors, Airmen and Marines are more valuable than any of the weapons systems the U.S. military will ever field. A successful Antiterrorism/Force Protection (AT/FP) program depends heavily on the fitness of those personnel assigned. Force Health Protection measures are to ensure a healthy and fit force is fielded in support of the AT/FP mission. The following are the basic requirements:
  - a.** Commanders at all levels are responsible for ensuring all U.S. military personnel stay current by receiving required immunizations, and following prescribed preventive medicine guidance and procedures.
  - b.** Personnel should encourage their family members to receive appropriate immunizations and to take the necessary precautions to stay healthy.
  - c.** All Commands must integrate medical support into their AT/FP plan to include mass casualty planning, Weapons of Mass Destruction (WMD) identification and control, food and water vulnerability assessments, and other appropriate preventive medicine measures.
  - d.** Additional information on Medical Services can be found on the USEUCOM Surgeon's Internet webpage at : <http://www.eucom.mil/hq/ecmd/prevmed/index.htm>.

#### ACKNOWLEDGE:

**JOSEPH W. RALSTON**  
General, USAF

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**Q-2**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**ANNEX X (DISTRIBUTION) TO USCINCEUR AT/FP OPORD 01-01**

Publication of this OPORD will be announced to all tasked organizations and supporting commands and agencies. The OPORD will be posted and available on the SIPRNET at the USEUCOM Force Protection Homepage under Publications. Additionally, copies will be provided on CD-ROM for use by Service component commands, U.S. Defense Representatives and other Direct Reporting Units.

**ACKNOWLEDGE:**

**JOSEPH W. RAWLSTON**  
**General, USAF**

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**X-2**  
**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****ANNEX Y (GLOSSARY) TO USCINCEUR AT/FP OPORD 01-01**

**1. GENERAL.** This glossary provides definition and interpretation for various Antiterrorism/Force Protection (AT/FP) terminology used in this order.

**2. APPLICATION.**

**a.** AT/FP terminology contained within this order complies as closely as possible with commonly used military terms defined in Joint Pub 1-02, The DoD Dictionary of Military and Associated Terms. However, the location/nomenclature used in this document may reflect USEUCOM AOR unique vocabulary.

**b.** Acronyms and Abbreviations employed will, in many cases, mirror the GENSER plain language address (PLA) database directory. Common terminology enhances the USEUCOM capability to identify, inform, and track DoD organizations and personnel subject to the requirements of this order.

**PART I — ABBREVIATIONS**

(C)	confidential
(S)	secret
(TS)	top secret
(U)	unclassified
AAR	after-action review
Admin	administrative
AFIS	American Forces Information Service
AFMC	Air Force Material Command
AFOSI	Air Force Office of Special Investigations
AFRTS	American Forces Radio/Television Service
AISC	Army Information Systems Command
AMC	Army Material Command
AMCIT	American citizen
AMEMBASSY	American Embassy
AOR	area of responsibility
APOD	aerial port of debarkation
APOE	aerial port of embarkation
ASAWG	Anti Terrorism Staff Working Group
ASD(PA)	Assistant Secretary of Defense for Public Affairs
ASD(SO/LIC)	Assistant Secretary of Defense for Special Operations/Low Intensity Conflict
AT	antiterrorism
ATO	Antiterrorism Officer
BDU	battle dress uniform
C2	command and control
CAA	command arrangements agreement

**FOR OFFICIAL USE ONLY**

CAT	crisis action team
CbT	Combating Terrorism
CbTRIF	Combating Terrorism Readiness Initiative Fund
CCC	Component Commanders Conference
CCTV	closed circuit television
CDC	concept development conference
CI	counterintelligence
CID	criminal investigative division
CINC	Commander in Chief
CISO	counterintelligence support officer
CIV	civilian
CIWG	counterintelligence working group
CJCS	Chairman Joint Chiefs of Staff
CMD	command
CMRT	Consequence Management Response Team
CO	Company
COCOM	combatant command
COE	Corps of Engineers
COM	Chief of Mission
Comm	communications
CONPLAN	operations plan in concept format
CONUS	continental United States
CoS	Chief of Staff
COS	Chief of Station
CRYPTO	cryptologic
CT	counterterrorism
CTF	Combined Task Force
CW	chemical warfare
DA	Department of the Army
DAO	Defense Attaché Office
DATT	Defense Attaché
DCINC	Deputy, Commander in Chief
DET	detachment
DIA	Defense Intelligence Agency
Dir	directive
DIRLAUTH	direct liaison authorized
DIWS	Defense Indications and Warnings System
DLA	Defense Logistics Agency
DoD	Department of Defense
DoDEA	Department of Defense Education Activity
DoDDS	Department of Defense Dependent School System
DON	Department of Navy
DOS	Department of State
DSCA	Defense Security Cooperation Agency
DTRA	Defense Threat Reduction Agency
EAC	emergency action committee



**FOR OFFICIAL USE ONLY**

EAP	emergency action plan
EEFI	essential elements of friendly information
EMR	embassy maintained residences
EOD	explosive ordnance disposal
ETCC	European Theater Command Center
ECIG	USEUCOM Inspector General
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEST	Foreign Emergency Support Team
FHP	Force Health Protection
FOUO	for official use only
FP	force protection
HAV	heavy armored vehicle
HN	host nation
HNG	host nation government
HQ	headquarters
HRP	high risk personnel
IAW	in accordance with
IG	inspector general
INTEL	intelligence
IO	Information Warfare
IPC	initial planning conference
ISOPREP	Isolated Personnel Reports
JAC	joint analysis center
JCET	Joint
JCS	Joint Chiefs of Staff
JIB	joint information bureau
JIC	joint intelligence center
JMETL	joint mission essential task list
JTF	joint task force
JTTP	joint tactics, techniques, and procedures
LAV	light armored vehicle
LGF	local guard force
LNO	liaison officer
LOI	letter of instruction
MAP	military assistance program
MCC	military coordinating committee
MEU	Marine Expeditionary Unit
MEU (SOC)	MEU (Special Operations Capable)
MI	military intelligence
MILGP	(U.S.) military group
MLO	military liaison office
MLT	Military Liaison Team
MNF	multi-national force
MOA	memorandum of agreement
MOOTW	military operations other than war

**FOR OFFICIAL USE ONLY**

MOPP	mission oriented protective posture
MOU	memorandum of understanding
MP	military police
MPC	mid-planning conference
MSC	Military Sealift Command
MSG	Marine Security Guards
MSGR	Marine security guard residence
MTMC	Military Transportation Management Command
NBC	nuclear, biological, chemical
NCIS	Naval Criminal Investigative Service
NEO	non-combatant evacuation order
NIST	National Intelligence Support Team
NMCC	National Military Command Center
NMR	news media representatives
NSA	National Security Agency
ODC	Office of Defense Cooperation
ODR	Office of Defense Representative
OMC	Office of Military Cooperation
OPCON	operational control
OPLAN	operations plan
OPORD	operations order
OPR	office of primary responsibility
OPSEC	operations security
OSPB	Overseas Security Policy Board
PA	public affairs
PAO	public affairs officer
PCS	Permanent Change of Station
PM	provost marshal
POC	point of contact
POLAD	political advisor
POR	principal officers residence
PPE	personal protective equipment
PSO	personal security officer
QRF	quick response force
REF	reference
ROE	rules of engagement
RSO	regional security officer
SAO	security assistance organization
SAV	staff assistance visit
SCI	special compartmented information
SECDEF	Secretary of Defense
SECSTATE	Secretary of State
SIPRNET	Secure Internet Protocol Router Network
SJS	Secretary of Joint Staff
SOCEUR	Special Operations Command, Europe
SP	security police

Y-4

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

SPOD	Seaport of debarkation
SPOE	Seaport of embarkation
SRWF	shatter resistant window film
SVC	service
TACON	tactical control
TAD	temporary additional duty
TCN	third country national
TDY	temporary duty
THREATCON	threat condition (Obsolete Term – Replaced by Terrorist Force Protection Condition)
TSPS	Theater Security Planning System
USC	U.S. Code
USEUCOM	United States European Command
USCINCEUR	Commander in Chief, U.S. European Command
USDAO	U.S. Defense Attaché Office
USDR	U.S. Defense Representative
USG	United States government
USIS	U.S. Information Service
USTRANSCOM	U.S. Transportation Command
VA	vulnerability assessment
VAMP	Vulnerability Assessment Management Program
VTER	A program code for antiterrorism funds.
WMD	weapons of mass destruction

**PART II — DEFINITIONS**

**ANTITERRORISM (AT).** Includes *defensive* measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces (Ref: Joint Pub 3-07.2).

**ANTITERRORISM/FORCE PROTECTION (AT/FP) PLAN.** An AT/FP Plan is the specific measures taken to establish and maintain a comprehensive AT Program which encompasses Force Protection.

**ANTITERRORISM (AT) PROGRAM.** The AT program is one of several security-related programs that fall under the overarching Force Protection and Combating Terrorism programs. An AT Program is a collective effort which seeks to reduce the likelihood that Department of Defense affiliated personnel, their families, facilities, and materiel will be subject to a terrorist attack, and to prepare to respond to the effects of such attacks should they occur.

**ANTITERRORISM OFFICER (ATO).** The installation and/or regional AT/FP advisor charged with managing the AT/FP Program for the commander. (Formerly referred to as the AT/FP Officer, or FPO.)

**FOR OFFICIAL USE ONLY**

**ASYMMETRIC WARFARE.** Unanticipated or non-traditional approaches to circumvent or undermine an adversary's strengths while exploiting his vulnerabilities through unexpected technologies or innovative means. Asymmetric warfare is defined from the vantage point of the target and focuses on vulnerabilities not appreciated by the target. Asymmetric warfare relies on concepts that are fundamentally different from the way the target fights. These concepts are designed to result in disproportionate leverage or advantage for the attacker by generating confusion, thus forcing the target to cede the initiative and/or lose the will to continue.

**COMBATING TERRORISM (CbT).** Combating terrorism within the Department of Defense encompasses all actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts), counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident/event), and intelligence support (collection and dissemination of terrorism-related information) taken to oppose terrorism throughout the entire threat spectrum, to include terrorist use of chemical, biological, radiological, nuclear materials or high-yield explosive devices (CBRNE) (Ref: Joint Pub 3-07.2).

**COUNTERTERRORISM (CT).** Involves *offensive* measures taken to prevent, deter, and respond to terrorism. Sensitive and compartmented counterterrorism programs are addressed in relevant National Security Decision Directives (NSDDs), National Security Directives (NSDs), contingency plans, and other relevant classified documents (Ref: Joint Pub 3-07.2).

**COUNTERINTELLIGENCE (CI).** Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (Ref: Joint Pubs 1-02 and 2-01.2).

**CRITICAL INSTALLATIONS.** From a DoD infrastructure perspective, critical installations are those defined as containing assets essential to planning, mobilization, deployment, and sustainment of military operations, whose loss or degradation jeopardizes the ability to the mission. Criticality, when viewed from a force protection perspective clearly goes further, as it seeks to prevent terrorist actions that would cause mass casualty events (Ref: Joint Pub 1-02).

**DEFENSE AGENCY.** A DoD organization operating within the USEUCOM AOR that is not assigned to, nor commanded by USCINCEUR or a component command, for example, the Defense Logistics Agency (DLA).

**FOR OFFICIAL USE ONLY****DEPARTMENT OF DEFENSE (DoD) TERRORISM THREAT ANALYSIS**

**METHODOLOGY.** See DoD O-2000.12-H for an explanation of the DoD Terrorism Threat Analysis Methodology.

**EMERGENCY ACTION COMMITTEE (EAC).** An organization established at a Foreign Service post by the Chief of Mission or principal officer, for the purpose of planning and coordinating the post's response to contingencies.

**ENGINEERING RELATED DEFINITIONS.** See Appendix 1, Annex D for definition of terms related to design construction standards.

**FORCE HEALTH PROTECTION (FHP).** Measures to mitigate both known and anticipated enemy and other health-related threats resulting from infectious disease, environmental exposures, combat stress, and non-battle injuries which hinder achievement of operational objectives in a given environment. The FHP concept promotes a healthy, fit, and medically ready force, strengthened against disease, illness, and injury through a continuous health surveillance program and emphasizes disease prevention, environmental surveillance, and health promotion as keys to maintenance and deployment of a robust force.

**FORCE PROTECTION (FP).** A security program designed to protect military personnel, civilian employees, family members, facilities, and equipment in all locations and situations. This is accomplished through planned and integrated application of combating terrorism, physical security, operations security (OPSEC), personal protective services, supported by intelligence, counterintelligence, and other security programs (Ref: Joint Pub 3-07.2).

**FULLY ARMORED VEHICLE (FAV) or non-tactical HEAVY ARMORED VEHICLE (HAV).** A high cost commercially manufactured vehicle designed to afford maximum protection to the occupants against high velocity ballistic threats as defined by the DoD FAV technical specifications. A FAV or HAV can originate from one of two sources: a commercial vehicle specifically designed, engineered, and manufactured to be a FAV/HAV; or a commercial vehicle modified by a commercial armoring firm, not the original manufacturer, to make the vehicle comply fully with the DoD technical specifications for a FAV.

**HIGH-RISK BILLET.** U.S. military or civilian personnel and their family members whose grade, assignment, travel itinerary, symbolic value and/or relative isolation make them especially attractive or accessible terrorist target. Rank and grade are not the sole determinant for designation as a high-risk person. Other key factors include, but are not limited to, vulnerabilities resulting from the individual's duties or inherent authorized personnel billet (identified and recommended by appropriate authority) that because of grade, assignment, travel itinerary, or symbolic value may make personnel filling them an especially attractive or accessible terrorist target.

## FOR OFFICIAL USE ONLY

**HIGH-RISK PERSONNEL (HRP).** U.S. personnel, who, by their grade, assignment, or symbolic value, are likely to be attractive or accessible terrorist targets.

**HIGH-RISK TARGETS.** U.S. material resources and facilities are often attractive and/or accessible terrorist targets because of mission sensitivity, ease of access, isolation, or symbolic value.

**LIGHT ARMORED VEHICLE (LAV).** A commercially manufactured vehicle modified to provide a level of protection to the occupants against medium/low ballistic threats as defined in the DoD LAV technical specifications.

**LONG TERM LEASE.** The leasing of an NTAV for 60 days or more for security purposes.

**NON-TACTICAL VEHICLE (NTAV).** A commercially manufactured vehicle (sedan, limousine, truck, bus, van, and/or sport utility vehicle, etc.) constructed or modified to provide ballistic protection to the occupants. There are two classes of NTAVs: Fully Armored Vehicles (FAV) and Light Armored Vehicles (LAV).

**OPERATIONS SECURITY (OPSEC).** A process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to:

- (1) Identify those actions that can be observed by adversary intelligence systems.
- (2) Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
- (3) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation (Ref: Joint Pub 3-07.2).

**PARTIALLY-ARMORED VEHICLES.** These vehicles, also referred to as kit cars, are hereafter referred to as non-tactical light armored vehicles (LAVs). LAVs are motor vehicles obtained through normal procurement channels to fulfill valid transportation requirements, and which are later altered by affixing armoring materials to the windows and body.

**PHYSICAL SECURITY.** That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft (Ref: Joint Pub 1-02).

**SHORT TERM LEASE.** The leasing of an NTAV for 59 days or less for security purposes.

**FOR OFFICIAL USE ONLY**

**TERRORISM.** The calculated use of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

**TERRORIST.** An individual, or group, who utilizes violence, terror, and intimidation to achieve a result.

**TERRORIST INCIDENT RESPONSE MEASURES.** A set of procedures in place for response forces to deal with the effects of a terrorist incident.

**TERRORISM CONSEQUENCE MANAGEMENT (TCM).** Department of Defense preparedness and response for mitigating the consequences of a terrorist incident including the use of a weapon of mass destruction. Department of Defense consequence management activities are designed to support the lead federal agency (domestically, FEMA; overseas, DOS) and include measures to alleviate damage, loss of life, hardship or suffering caused by the incident; protect public health and safety; and restore emergency essential government services.

**TERRORISM THREAT ASSESSMENT.** The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat, and the product of a threat analysis for a particular unit, installation, or activity.

**THREAT ANALYSIS.** In the context of antiterrorism, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target a facility. A threat analysis will review the factors of the presence of a terrorist group, operational capability, activity, intentions, and operating environment.

**TERRORIST FORCE PROTECTION CONDITIONS (also referred to as Force Protection Conditions or FPCON, and formerly known as THREATCON).** A DoD-approved system standardizing the Department's identification of and recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. The system is the principle means for a commander to apply an operational decision on how to protect against terrorism and facilitates inter-Service coordination and support for antiterrorism activities. Under this system, specific protective security (often referred to as Antiterrorism/Force Protection (AT/FP)) measures are identified to be taken under each Force Protection Condition. There are five associated Force Protection Condition definitions:

**(1) FORCE PROTECTION CONDITION NORMAL.** This condition exists when a general **global** threat of possible terrorist activity exists **and** warrants a routine security posture.

**(2) FORCE PROTECTION CONDITION ALPHA.** This condition applies when there is a general threat of possible terrorist activity against personnel **or** facilities, the

**FOR OFFICIAL USE ONLY**

nature and extent of which are unpredictable. ALPHA measures must be capable of being maintained indefinitely.

**(3) FORCE PROTECTION CONDITION BRAVO.** This condition applies when an increased and more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and relations with local authorities.

**(4) FORCE PROTECTION CONDITION CHARLIE.** This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel or facilities is likely. Implementation of CHARLIE measures will create hardship and affect the activities of the unit and its personnel.

**(5) FORCE PROTECTION CONDITION DELTA.** This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods.

**TERRORISM THREAT LEVEL.** An intelligence threat assessment of the level of terrorist threat faced by U.S. personnel and interests in each of the Command's AOR countries. See Annex B for detailed discussion. USEUCOM threat levels should not be confused with Force Protection Conditions.

**TRANSNATIONAL THREAT.** Any extra-governmental activity/organization that transcends national borders and threatens the national security of the United States. A "Transnational Threat" may employ asymmetric means (acts of terrorism) as a tool, but is not the same as an "Asymmetric Threat."

**USEUCOM ACTIVITY.** Any detachment, unit, office, force or component under the operational control of operational command of USCINCEUR.

**U.S. DEFENSE REPRESENTATIVE (USDR).** The USDR is the in-country representative of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the geographic Commander of the Unified Command for coordination of security matters for all in-country noncombatant DoD elements (i.e., those DoD personnel and organizations not assigned to, or attached to, and under the command of a combatant commander).

**VTER FUNDS.** A Management Decision Package (MDEP) program that provides funding for projects that protect personnel, facilities, and equipment from terrorist/criminal threats. Reduces unit and installation vulnerability during higher levels of threat. VTER is not an acronym, but a program code.



**FOR OFFICIAL USE ONLY**

**VULNERABILITY.** In antiterrorism, a situation or circumstance, if left unchanged, that may result in the loss of life or damage to mission essential resources. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or will to fight diminished. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.

**VULNERABILITY ASSESSMENT.** The process through which the Commander determines the susceptibility to attack from the full range of threats to the security of personnel, family members, and facilities, which provides a basis for determining antiterrorism measures that can protect personnel and assets from terrorist attacks.

**WARDEN NOTIFICATION SYSTEM.** A Department of State system of person-to-person communication used to relay information, alerting orders, or directives to Embassy personnel and other U.S. citizens.

**WEAPONS OF MASS DESTRUCTION.** Any weapons or device that is intended, or has the capability of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Can be nuclear, chemical, biological, radiological, or large explosive device weapons, but excludes the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

**ACKNOWLEDGE:**

**JOSEPH W. RALSTON**  
**General, USAF**

**FOR OFFICIAL USE ONLY**

(INTENTIONALLY BLANK)

**Y-12  
FOR OFFICIAL USE ONLY**