k. Measure 51. Spare for MACOM or installation use.

APPENDIX C
Management Control Evaluation Checklist

C-1. Function

The function covered by this checklist is the management of unit AT/FP Programs.

C-2. Purpose

The purpose of this checklist is to assist assessable commanders in evaluating the key management controls outlined below. It is not intended to cover all controls. Questions raised in this appendix are for checklist purposes only and should not be construed as an independent basis for authority to act in response to any particular question. Any such response must comport and comply with applicable statute and regulation.

C-3. Instructions

Answers must be based on the actual testing of key management controls (e.g., document analysis, direct observation, sampling, simulation, exercise, other). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key management controls must be formally evaluated at least annually IAW paragraph 5-8. Certification that this evaluation has been conducted must be accomplished on DA Form 11-2-R (Management Control Evaluation Certification Statement).

C-4. Test Questions

a. Army Standard 1. Commanders will develop a full working knowledge of AT/FP policies. Further, they will communicate the spirit and intent of these policies throughout the chain of command or line of authority. MACOMs are responsible for development of subsequent MACOM unique and prescriptive physical security standards. Questions:
   (1) Has the MACOM published a supplement to AR 525-13, implementing guidance, or an operations order outlining MACOM unique and prescriptive physical security requirements?
   (2) If a supplement to AR 525-13 or operations order was published was it approved by HQDA?

b. Army Standard 2. Assignment of AT/FP Operational Responsibility: Commanders will establish clear operational responsibility for AT/FP for all units and individuals whether permanently or temporarily assigned. Questions:
   (1) Are procedures in place to ensure each individual and unit is aware of who is operationally responsible for AT/FP?
(2) Are procedures in place to ensure those personnel operationally responsible for AT/FP are notified upon the arrival and departure of individuals and units?

C. Army Standard 3. AT/FP Program and Planning: AT/FP programs will be based on assessments of threats and vulnerabilities. AT/FP operational planning will identify, coordinate, allocate, and employ resources to ensure AT/FP measures are developed that provide the appropriate level of protection for all applicable threats. Questions:

(1) Does the command have an established AT/FP program with implementing plans and guidance?
(2) Are plans based on a published threat and vulnerability assessments?
   (a) Does planning coordinate and synchronize the AT/FP plan and supporting annexes?
   (b) Is AT/FP included in all phases of deployment planning?
   (c) Are tenant units included in planning?
(3) Do interservice support agreements, MOU, and MOA consider AT/FP?
(4) Does the command monitor the effectiveness of the AT/FP programs at subordinate commands/units? Are deficiencies and corrective actions identified, documented, and tracked?
(5) Is there a current Physical Security Plan IAW AR 190-13 approved by the commander?
   (a) Does the plan contain the basic requirements IAW AR 190-13 (e.g., bomb threat, installation closure, threat statement, etc.)?
   (b) Are the components of the plan tested IAW AR 190-13?
   (c) Is the process of risk analysis/management well defined, understood, and incorporated into physical security planning and execution?
(6) Does the installation/unit possess a terrorist incident response plan?
(7) Does the installation have a plan to conduct post incident response? Has it been tested in conjunction with the terrorist response plan?
(8) Does the installation have plans and procedures in place to reconstitute after a terrorist attack? Has that portion of the plan been tested?
(9) Are emergency evacuation plans in-place and are they tested?
(10) Is there an attack warning system which utilizes a set of recognizable alarms with reactions to potential emergencies, as determined by the threat and vulnerability assessment? Are personnel trained and proficient in recognition?

d. Army Standard 4. Committees and Working Groups: Commanders will establish AT/FP committees to assist in the development, integration, and management of the AT/FP program. Additionally, commanders will establish AT/FP working groups. AT/FP working groups should meet frequently to discuss the threat and evaluate security measures planned or implemented. AT/FP working groups will operate under the direction of the command AT/FP officer to develop issues for presentation to the AT/FP committee. Questions:

(1) Does the AT/FP committee meet at least semi-annually?
(2) Do all of the personnel required by AR 525-13 and the commander sit on the committee (e.g., operations, PM/SO, intelligence, information management, engineer, logistics, medical, budget, SJA, USACIDC, chemical, public affairs, etc.)?
(3) Does the AT/FP committee provide the commander with a written record of the meetings and maintain those records on file?

(4) Does the AT/FP working group meet frequently during times of increased threat?

(5) Does the AT/FP working group develop issues for presentation to the command's AT/FP committee?

e. Army Standard 5. Exercises: Commanders will institute an exercise program which develops and refines the command's AT/FP procedures and responses to the entire spectrum of AT/FP threats. Questions:

(1) Is there a system in place to exercise AT/FP related plans and attack warning systems at least annually?

(2) Do the scenarios involve the staff (that have AT/FP responsibilities)?

(3) Is there a feedback mechanism to route after action review results through the AT/FP committee to the commander?

(4) Is OPSEC considered in the planning, conduct, and evaluation of exercises?

f. Army Standard 6. Risk Management: The Army 5-step risk management process will be integrated into all AT/FP related planning and program execution. Questions:

(1) Do the commander and staff understand the Army 5-step risk management process?

(2) Is risk management incorporated into all AT/FP planning and program execution by both the commander and staff?

(3) Is risk management considered in all elements of the AT/FP program (e.g., physical security, information operations, resource management, etc.)?

g. Army Standard 7. Periodic Program Review: Installation AT/FP programs will be reviewed by their MACOM at least once every three years. Questions:

(1) Have installation programs been reviewed by MACOMs within the last three years?

(2) Were the inspection results documented?

(3) Were deficiencies corrected?

h. Army Standard 8. AT/FP Officer: Commanders will designate a AT/FP officer. The AT/FP officer will be assigned to the operations section. Questions:

(1) Has the commander appointed an AT/FP officer on orders?

(2) Does the AT/FP officer have direct access to the commander?

(3) Is the AT/FP officer certified and current?

i. Army Standard 9. Development of Local Threat Conditions Levels: Commanders will develop a process based on threat information and/or guidance from higher headquarters to raise or lower THREATCON levels. THREATCON transition procedures and measures will be disseminated and implemented by all subordinate and tenant commanders. Questions:

(1) Is there a process in place to change THREATCON levels, when required?

(2) Has the process been tested within the past year?

(3) Are there sufficient assets to implement all THREATCONs? If not, are there procedures to:

(a) Divert/acquire local assets on an emergency basis consistent with the Federal Acquisition Regulation?
(b) Notify higher headquarters of shortfalls?
(4) Are enhanced security measures planned for post housing areas in the event of a heightened THREATCON?
(5) Is there a process to continuously review the effectiveness of physical security measures under THREATCON Normal?

j. Army Standard 10. Weapons of Mass Destruction Planning: AT/FP plans, orders, SOPs, threat assessments, and coordination measures will address potential threat use of WMD. Commanders will assess the vulnerability of installations, facilities, and personnel within their AOR to threat use of WMD. Clear command, control, and communication lines will be established between local, state, Federal, and host nation emergency assistance agencies to detail support relationships and responsibilities.

Questions:

(1) Is the threat use of WMD assessed?
(2) Is WMD included in the crisis management plan?
(3) Does this plan address potential threats and vulnerability assessments?
(4) Are probable WMD targets identified?
(5) Are plans coordinated with local, state, Federal, and HN authorities and do they participate in exercises?
(6) Do staff duty instructions include WMD threat response procedures?
(7) Is there a WMD attack warning system and are procedures established and exercised to proficiency?
(8) Are there provisions to establish rapid communications between military, local, state, Federal, and host nation agencies?

k. Army Standard 11. First Response and Consequence Management: First responders will be officially identified, trained, and equipped to respond to both conventional and WMD attack. Detailed response plans will include: casualty triage, decontamination, evacuation, and tracking; site security, evidence preservation, and contamination control measures; and detailed interagency support and coordination measures. Annual AT/FP exercises will test medical response and consequence management procedures, including WMD response measures. Questions:

(1) Are first responders officially designated?
(2) Are first responders trained to respond to conventional and WMD attacks?
(3) Do first responders have adequate protective equipment, including chemical defense equipment?
(4) Are emergency first responder equipment shortfalls considered in AT/FP planning?
(5) Are local hospitals capable of treating mass casualties, including WMD casualties and have MOAs or MOUs been established to do so?
(6) Are patient decontamination responsibilities assigned in AT/FP plans?
(7) Are location and status of casualties tracked?
(8) Are medical MASCAL and WMD scenarios included in the AT/FP exercise program?
(9) Are installation staffs integrated into WMD/MASCAL training?
(10) Is the PA0 a participant in MASCAL and WMD exercises?
(11) Are adequate resources available to support the emergency response plan?
(12) Do WMD response plans address mass casualty scenarios in high density population areas?

I. Army Standard 12. Command Information Program: Commanders will incorporate AT/FP into their command information programs. Questions:

(1) Does the commander incorporate AT/FP Program information into the command information program?

(2) Is AT/FP information being effectively disseminated through multiple means (e.g., briefings, posters, newspaper/newsletter articles, chain of concern, radio, and television)?

(3) Is AT/FP information formatted for the Total Army (soldiers, family members, DA civilians)?

(4) Is OPSEC included in all public affairs operations?

m. Army Standard 13. Collection of AT/FP Intelligence Information: Commanders will have a fully integrated foreign, domestic, and criminal intelligence AT/FP intelligence program focused and based on PIR that provides the appropriate threat information to protect personnel, family members, facilities, and material in all locations and situations. The commander will ensure production and analysis requirements are focused and based on PIR. Questions:

(1) Are military intelligence collection operations being conducted consistent with the requirements of AR 381-10 and other applicable regulations and directives?

(2) Are law enforcement collection operations being conducted consistent with the requirements of AR 380-13, DoDD 5200.27, and other applicable regulations and directives?

(3) For CONUS commanders, is this full integration conducted outside the intelligence office IAW the limitations of AR 381-10 and other applicable regulations and directives?

(4) Does the command have connectivity to receive threat related information from all available sources (e.g., FBI, local law enforcement, Intelink-S, and Intelink)?

(5) Is the activity familiar with the ACIC and does it know how to obtain ACIC products?

(6) Is the activity receiving the MITS?

(7) Has the commander established PIR?

(8) Are the commander's PIR the basis for production requirements?

(9) Are there sufficient sensitive compartmented information (SCI) billets to support the mission?

(10) Is the DoD Terrorist Threat Level Classification system utilized to identify the threat in a specific overseas country?

n. Army Standard 14. Threat and Vulnerability Assessments: Commanders will prepare threat and vulnerability assessments for their AOR. Questions:

(1) Have multi-disciplined threat and vulnerability assessments been conducted?

(2) Is the entire spectrum of threats, to include threat use of WMD, part of the threat and vulnerability assessments?

(3) Are the results of the threat and vulnerability assessment reviewed and used as part of the commander's criteria for setting specific THREATCON measures?
(4) Are the results of the threat and vulnerability assessment disseminated to affected organizations (e.g., organic, tenant, and supported RC units)? Where specific vulnerabilities are identified are they reviewed for appropriate classification?

(5) Is the ACIC utilized as a tool to conduct foreign threat assessments?

(6) Are procedures in place to conduct follow-on threat and vulnerability assessments of deployed forces?

o. Army Standard 15. Dissemination of AT/FP Intelligence Information: Commanders will ensure AT/FP intelligence information is disseminated in a timely manner. Current intelligence will be integrated into the AT/FP training program.

Questions:

(1) Is threat information being coordinated with other staff elements involved in the AT/FP program?

(2) Are procedures in place to disseminate threat information and intelligence products to higher/subordinate activities and tenant organizations (during duty and non-duty hours)?

(3) Is the “no double standard policy” (threat information distributed to military, civilian, and contractor workforce) followed/understood when disseminating threat information?

p. Army Standard 16. Individual Training: Commanders will ensure all military and DA Civilian personnel in their command receive the appropriate training for individual antiterrorism awareness prior to deploying or traveling outside the 50 United States, its territories, and possessions. Units will maintain a record of individuals receiving training. Family members will receive similar training prior to traveling outside the 50 United States, its territories, and possessions when on official Government orders.

Questions:

(1) Do policies and guidance ensure personnel (military, DA civilians, and family members) are provided with the appropriate level of AT training, education, and awareness?

(2) Is the command aware of Army requirements for Levels I and II AT training and have they implemented the program?

(3) Does the program train all personnel in AT/FP procedures, guidance, and regulations?

(4) Does AT awareness training incorporate the postulated threat?

(5) Are theater specific predeployment requirements for the CINC AORs being accomplished?

(6) Is there a validation process to ensure Level I training is accomplished for deployments, PCS, TDY, and leave/pass?

(7) Is the DoD list of high-threat and potential physical threat countries maintained and disseminated throughout the command?

(8) Are AT/FP training materials readily available (e.g., Level I videos, GTA wallet cards, etc.)?

(9) Are personnel with specific AT/FP duties sent to required courses in accordance with applicable regulations?

q. Army Standard 17. Leader Training: Individuals identified as having significant responsibilities for the command AT/FP program will receive adequate training that
provides them with the ability to train others, as well as advise the commander. 

Question: Are key leaders with AT/FP responsibilities trained?

r. Army Standard 18. Hostage Training: Personnel assigned to medium or high terrorist threat level areas, will receive guidance at least annually on appropriate conduct in the event they are taken hostage or kidnapped. Question: Is training being conducted by a certified and current instructor?

s. Army Standard 19. Training in Support of High Risk Personnel. Commanders will ensure HRP and their family members are made aware of risks and trained in personal protective measures. Additionally, support staff such as drivers, aides, and protective services details will be trained and equipped. Questions:

(1) Is evasive driving training offered to HRP and their drivers as necessary to counter the assessed threat and vulnerabilities identified in the PSVA?

(2) Is training in supplemental individual protective measures provided to HRP?

(3) Is similar awareness training offered to the families of HRP?

(4) Is awareness training provided to support staff such as drivers and aides?


U. Army Standard 21. C2 Protect Integration and Training: Commanders will ensure C2 Protect is integrated into all AT/FP planning and program execution, and supporting training is planned for and resourced. Commanders will ensure integration of, and adherence to, relevant laws and regulations pertaining to security of the command's information infrastructure. Questions:

(1) Have the provisions of AR 380-19 governing the use of automated tools to conduct assessments and analysis for continuity of operations integrated into the command's AT/FP program?

(2) Have the provisions of AR 380-53 governing security monitoring, exploitation, and penetration activities been adhered to and integrated into the command's AT/FP Program?

(3) Are the following components of C2 Protect and AR 25-XX (when published) being integrated into the AT/FP Program?
(a) OPSEC?
(b) Electronic security?
(c) Physical security?
(d) Intelligence?
(e) ISS?
(f) Counter-deception?
(g) Counter-PSYOPS?

(4) When incidents occur on the network are they reviewed and trends developed indicating significant weaknesses?
(5) Are C2 Protect representative active participants on the command AT/FP committee?
(6) Are incident reporting procedures published for system administrators IAW AR 380-19, AR 25-XX (when published), and ACERT reporting procedures?
(7) Has a warning system been devised to alert the command of incidents?
(8) Is the command familiar with the roles of the LIWA/ACERT?
(9) Does the OPSEC plan include the provisions of AR 530-1? Are OPSEC threats identified? Is OPSEC part of the unit training program?
(10) Are C2 Protect components included in threat briefings and assessments provided to the command, as appropriate?
(11) Is there a computer security awareness program?
(12) Does the command monitor the effectiveness of C2 Protect integration at the subordinate command and unit level?
(13) Are system administrators and network administrators trained IAW AR 380-19?
(14) Does the available training meet program requirements?
(15) Is information system security training provided to the user IAW AR 380-19?
(16) Is there a training plan developed to ensure continual operations in event of major disruptions IAW AR 380-19?
(17) Are all personnel trained and familiar with their OPSEC responsibilities IAW AR 530-1?
(18) Are appropriate security personnel appointed and trained (e.g., ISSO, TASO, or NSO)?

v. Army Standard 22. C2 Protect Threat and Vulnerability Assessments:
Commanders will ensure friendly information systems are included in threat and vulnerability assessments. Commanders will ensure C2 Protect procedures and techniques are developed to protect the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. Questions:
(1) Is the command registered in the Terminal Server Access Controller System for access to the Army tool set and are requirements for tools identified?
(2) Are procedures to report incidents to the ACERT in place and incidents reported?
(3) Do network operators obtain assistance installing security patches (fixes to vulnerabilities) from the ACERT?
(4) Are Defense Information Systems Agency Automated System Security Incident Support Team Bulletins received by all system and network administrators?

(5) Has the OPSEC process been applied in determining threats and vulnerabilities to your communications infrastructure?

(6) Are ISS procedures routinely reviewed and tested (e.g., user IDs, passwords, audit trails, and system configurations)?

(7) Is information systems security training performed at appropriate levels?

(8) Are security incidents/violations (e.g., viruses, unauthorized entries or attempts, and password compromises) analyzed, reviewed, investigated, and reported IAW AR 380-19, AR 25-XX (when published), and ACERT reporting procedures?

(9) Are security measures employed to control the external access? (e.g., callback and tokens)

(10) Is an automated audit capability (i.e., log security-related events) available and used in all systems?

(11) Is identification and authentication (i.e., user id/password, biometric devices, and tokens) required for access to all systems?

(12) Was the OPSEC process applied in developing countermeasures for the communication infrastructures?

(13) Are vulnerability assessments performed on the Army communications infrastructures by authorized U.S. Army activities or approved contractors using U.S. citizens only?

(14) Are countermeasures identified and in place based on the results of vulnerability assessments?

(15) Is there a written security plan to document implementation of countermeasures?

(16) Are sufficient secure communications available to the command?

w. Army Standard 23. Security Engineering and Employment of Security Measures: AT/FP will be considered in standard Army design practice with security measures based on risk and threat analysis. Questions:

(1) Are physical security and THREATCON considerations incorporated into the installation master plan and site selection?

(2) Are the results of vulnerability assessments incorporated into the installation military construction design program?

(3) Are risk analyses performed and AT/FP measures considered for all new and existing facilities either designated or likely to be designated MEVAs?

(4) Are local engineers familiar with the resources (such as the Protective Design Center and the Electronic Security Systems Center) available to them in security engineering?

(5) Are detection and assessment measures integrated with defense (delay) measures to protect personnel and material assets?

(6) Are security engineering surveys conducted when planning new facilities or renovating existing facilities?

(7) Was risk and threat analysis utilized in the development of any protective measures beyond those specifically requiring employment by regulation?
(8) Are TM's 5-853-1 through 5-853-4 used in the development and employment of security measures?

x. Army Standard 24. Mission Essential/Vulnerable Areas: MEVAs, which are critical to mission accomplishment or are vulnerable to theft/damage/attack, will be identified in order to focus security efforts. Questions:

(1) Are MEVAs identified, prioritized, and approved by the commander IAW AR 190-13?

(2) Are periodic reviews conducted IAW AR 190-13 to update areas designated as MEVAs?

(3) Are physical security inspections of MEVAs conducted IAW AR 190-13?

y. Army Standard 25. Restricted Areas: Areas which are considered critical or sensitive will be identified and formally designated as "Restricted Areas" in order to give commanders legal authority to impose special access controls. Questions:

(1) Are restricted areas identified and designated IAW AR 190-13?

(2) Are restricted areas correctly posted?

z. Army Standard 26. Random Antiterrorism Measures Program: Commanders will develop a Random Antiterrorism Measures Program (RAMP) for all Army installations and facilities that have the structures, equipment, personnel, and authority to control access. Questions:

(1) Does RAMP include a selection of different types of vehicle searches (trunk, undercarriage, total), document inspections, and observable security procedures designed to vary the look of the security program?

(2) Is RAMP thoroughly planned to ensure measures are implemented randomly (not in predictable patterns)?

(3) Does RAMP vary the types of measures along with schedules for employment of measures?

aa. Army Standard 27. Residential Security Assessment for Off-Post Housing: Commanders in medium or high terrorist threat level areas will conduct physical security assessments of off-post residences for permanently assigned and TDY personnel. Based on the assessment results, the individual may not be allowed to enter into a lease unless the facility owner takes certain measures. Questions:

(1) Are physical security assessments conducted on initial occupancy and annually thereafter?

(2) Is an up-to-date listing of residences for TDY and permanently assigned personnel maintained and safeguarded, and are they included in terrorist incident response plans?

bb. Army Standard 28. Facility and Site Evaluation/Selection Criteria: Commanders will develop a prioritized list of AT/FP factors for site selection teams. These criteria will be used to determine if facilities, either currently occupied or under consideration for occupancy, can adequately protect occupants against terrorist attack. Questions:

(1) Is there a prioritized list of AT/FP factors for site selection teams reviewed and approved by the commander?

(2) Is the list utilized?

cc. Army Standard 29. Law Enforcement Operations: Law enforcement operations will support installation AT/FP requirements through the commander's authority to
enforce Federal law and Army regulations. In the event of acts of terrorism on installations, military and DA police will take immediate action to resolve the incident and prevent loss of life. Terrorist incident response plans will include the use of law enforcement as first responders and provide procedures for employing police resources effectively. Questions:

1. Is the PM adequately resourced to conduct law enforcement operations in support of the installation AT/FP program?
2. Have adequate law enforcement contingency plans for emergency situations (e.g., bomb threats, hostage taking, base closures, and increased THREATCON levels) been developed and exercised?
3. Are exercise results provided to the commander through the AT/FP committee?
4. Has each command/activity supporting these plans been given the opportunity to participate in the creation of the plan and are they in receipt of a copy of the plan?
5. Do plans address backfill of law enforcement personnel during deployments?
6. Do PM/SO plans provide a detailed description of the employment for augmenting security forces and increased security force requirements for all THREATCON levels?

dd. Army Standard 30. Law Enforcement Liaison: PM/SO will conduct effective liaison with Federal, state, local, and HN agencies, as appropriate, to ensure criminal and terrorist intelligence is shared and plans and operations supporting AT/FP are coordinated. Questions:

1. Does coordination of security plans include applicable Federal, state, local, and host nation officials outlining movement, security, and jurisdictional responsibilities?
2. Is liaison conducted to ensure criminal intelligence, to include U.S. domestic threat information, is properly gathered, processed, and passed?
3. Is this information coordinated through the AT/FP committee process?
4. Are law enforcement operations coordinated with the appropriate Federal, state, local, and host nation agencies?

ee. Army Standard 31. Identification and Designation of High Risk Personnel: Commanders will ensure personnel who are at a greater risk than the general population, by virtue of their rank, assignment, symbolic value, vulnerabilities, location, or specific threat, are identified and assessed. Personnel requiring additional security to reduce or eliminate risks will be formally designated as HRP in order to make them eligible for special control/security measures. Questions:

1. Is there a formal procedure for designating HRP? Have HRP been designated?
2. Is there a periodic review of HRP designations?
3. If the MACOM delegated authority to installation for HRP designation is a written copy on-hand?

ff. Army Standard 32. Protective Measures for Safeguarding High Risk Personnel: Commanders will take appropriate measures to provide enhanced protection to HRP. Questions:

1. Are HRP receiving personal security vulnerability assessments from CID?
2. Are protective services details available to protect Level I HRP?
3. Are hardened cars available to support Level I HRP?
4. Have safe havens been established in quarters and offices?
(5) Are alarms installed in quarters and offices of HRP?
(6) Are working dogs available to conduct explosives detection sweeps?

C-5. Suppression

This is the first publication of this checklist.

C-6. Comments

Help to make this a better tool for evaluating management controls. Submit comments to: HQDA (DAMO-ODL-AT/FP), ODCSOPS, 400 ARMY PENTAGON, WASHINGTON, DC 20310-0400.

Appendix D
Required Reports

D-1. Terrorist Threat Report (TTR)

a. TTRs will be submitted utilizing the OPREP-3 format when a command receives credible information concerning a planned terrorist attack against U.S. Army personnel (soldiers, civilian employees, or their family members), facilities, or other assets. Information is "credible" if it is considered serious enough to warrant a THREATCON change or implementation of additional security measures which are targeted to counter a specific threat.

b. The OPREP-3 will be provided immediately by telephone to the Army Operations Center (AOC) (phone DSN 227-0218/9 or commercial (703) 697-0218/9). Local commanders will comply with any additional MACOM guidance concerning dissemination of such time-sensitive information.

c. A follow-up OPREP-3 will be transmitted within six hours of receiving the information by IMMEDIATE precedence electrical message to HQDA (DA WASH DC // DAMO-AOC/DAMO-ODL-AT/FP/ DAMO-ODO/DAMI-CHI//), USACIDC (CDRUSACIDC FT BELVOIR VA //CIOP-IN//), and INSCOM (CDRINSCOM FT BELVOIR VA //IAOPS-IS//). Local commanders will include their MACOM (and the MACOM with geographical responsibility for the location of the incident) as information addressees and comply with any additional MACOM guidance concerning dissemination of such information.

d. OPREP-3 updates should be submitted when additional substantive information concerning the terrorist threat becomes available. Such reports will be submitted within upon receiving the information by PRIORITY precedence electrical message directly from the command receiving the information to the addressees in para D-1.c. All information addressees for the initial OPREP-3 will be provided this and future updates.

e. The initial OPREP-3 will include date, time, and location and brief description of the threatened attack and response thereto.

f. Updates will provide additional information, as available, concerning the following:
   (1) Type of incident threatened.
   (2) Possible targets.