



DEPARTMENT OF THE NAVY
NAVY PERSONNEL COMMAND
5720 INTEGRITY DRIVE
MILLINGTON TN 38055-0000

NAVPERSCOMINST 5530.1E
PERS-534

24 AUG 2010

NAVPERSCOM INSTRUCTION 5530.1E

From: Commander, Navy Personnel Command

Subj: PHYSICAL SECURITY, LOSS PREVENTION, AND ANTI-TERRORISM

Ref: (a) OPNAVINST 5530.14E
(b) NAVSUPACTMIDSOUTHINST 5530.1E
(c) NAVSUPACTMIDSOUTHINST 5530.2D
(d) SECNAV M-5510.30 of 1 Jun 06
(e) SECNAV M-5510.36 of 1 Jun 06
(f) NAVSUPACTMFSINST 11320.3A
(g) NAVPERSCOMINST 5510.1B
(h) SECNAVINST 3300.2B
(i) OPNAVINST 3300.53A
(j) COMNAVPERSCOMINST 5000.1
(k) DoD O-2000.12-H of Feb 04

Encl: (1) NAVPERSCOM Physical Security and Anti-Terrorism/Force Protection (AT/FP) Plan
(2) Force Protection Conditions (FPCON)

1. Purpose. To establish policy, provide guidance, and set forth standards for physical security measures, key and lock control, fire prevention, loss prevention, and anti-terrorism for Bureau of Naval Personnel, Millington (BUPERS Millington)/ Navy Personnel Command (NAVPERSCOM). This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. NAVPERSCOMINST 5530.1D.

3. Discussion. An effective physical security program must receive attention and direction from all echelons within the chain of command, and properly trained and equipped personnel must carry out physical security functions. Security postures must be accurately assessed and resources provided to execute effective measures. References (a) through (k) and enclosures (1) and (2) provide the necessary guidance to physically safeguard government property and material at BUPERS Millington/ NAVPERSCOM.

24 AUG 2010

4. Responsibilities. Security is the direct, immediate, legal, and moral responsibility of all BUPERS Millington/NAVPERSCOM personnel (military, civilian, and government contract) assigned to BUPERS Millington/NAVPERSCOM. The NAVPERSCOM Security Manager (PERS-534) is responsible to the NAVPERSCOM Director, Command Support Services Division (PERS-53) for planning, implementing, enforcing, and supervising the physical security and loss prevention program of the command.

5. Action

a. All Bureau of Naval Personnel (BUPERS) Millington, Office of the Chief of Naval Operations (OPNAV), Personal Readiness and Community Support (N135), and NAVPERSCOM personnel (military, civilian, and government contract), regardless of rank, rate, or grade, assigned will comply with this instruction, the applicable requirements of references (a) through (k), and other directives issued by higher authority.

b. NAVPERSCOM (PERS-534) will coordinate with Naval Support Activity (NAVSUPACT) Mid-South Security regarding physical security and antiterrorism/force protection issues, intrusion detection systems, and the common access card (CAC) electronic access control system for NAVPERSCOM buildings.

6. Records Management. Records created by this instruction, regardless of media, will be managed per SECNAV M-5210.1 of September 2007.

7. Forms

a. The following forms are available from the NAVPERSCOM Security Manager or at <http://www.dtic.mil/whs/directives/> for DD 200, and <https://forms.daps.dla.mil/order/> for OPNAV forms.

(1) DD 200 (Oct 99), Financial Liability Investigation of Property Loss.

(2) OPNAV 5527/8 (12-82), Telephonic Threat Complaint.

NAVPERSCOMINST 5530.1E

24 AUG 2010

(3) OPNAV 5521/27 (Sep 92), Visitor Request/Visitor
Clearance Data.



ANN C. STEWART
Deputy Commander,
Navy Personnel Command

Distribution:

Electronic only, via NAVPERSCOM Web site
<http://www.npc.navy.mil/>

Copy to:

NAVSUPPACT Mid-South

**NAVY PERSONNEL COMMAND (NAVPERSCOM)
PHYSICAL SECURITY AND
ANTI-TERRORISM-FORCE PROTECTION (AT/FP) PLAN**

1. Area Security. The NAVPERSCOM Security Manager (PERS-534) is responsible for physical security in the following NAVPERSCOM office buildings located on NAVSUPPACT Mid-South.

Ray Hall	Bldg. 453
LT Clyde Everett Lassen Building	Bldg. 457
Goetsch Hall	Bldg. 768
Wood Hall	Bldg. 769
LT Vincent R. Capodanno Building	Bldg. 785
Captain John Phillip Cromwell Building	Bldg. 789
Jamie Whitten Building	Bldg. 791

2. Aids to Security

a. Protective Barriers. Physical barriers control, deny, impede, delay, and discourage access by unauthorized persons. NAVSUPPACT Mid-South Security controls gate access to the NAVSUPPACT Mid-South base.

b. Protective Lighting. Protective lighting increases the effectiveness of security forces, has considerable value as a deterrent to thieves, and may make the job of the saboteur or terrorist more difficult. Exterior lighting has been installed throughout NAVPERSCOM. These lights are operated by photoelectric cells or by manual switches. NAVSUPPACT Mid-South Public Works Officer is responsible for inspection and maintenance of all exterior protective lighting. Reference (b) provides additional information on the lighting for NAVSUPPACT Mid-South.

c. Intrusion Detection Systems (IDS)/Access Control System (ACS). IDS's are designed to detect, not prevent actual or attempted penetrations. The ACS installed in all NAVPERSCOM buildings is activated 24 hours a day. The ACS contributes to the overall physical security posture and the attainment of security objectives for NAVPERSCOM.

d. Communications. The primary means of communication within NAVPERSCOM are primarily the telephone and local area networks.

24 AUG 2010

Per reference (a), NAVSUPPACT Mid-South Security shall have its own communications system sufficient to maintain sure and rapid communication requirements throughout emergencies.

e. Closed Circuit Television (CCTV). CCTV surveillance systems are installed on all NAVPERSCOM buildings. The CCTV consists of 57 cameras and 4 digital video recorders/monitors that record all movement 24 hours a day. The CCTV cameras are installed at all entrance and exit doors and provide additional security for loss prevention.

3. Security Forces. NAVSUPPACT Mid-South Security is responsible for the perimeter security of all NAVPERSCOM buildings. An auxiliary security force (ASF) is composed of local, non-deploying military personnel permanently assigned to NAVSUPPACT Mid-South and tenant commands. The ASF is used to augment the NAVSUPPACT Mid-South Security Force during increased Force Protection Conditions (FPCONS) or when directed by NAVSUPPACT Mid-South. When the ASF is activated, BUPERS Millington/NAVPERSCOM personnel are under the cognizance of the NAVSUPPACT Mid-South Security Officer. Per references (a), (b), and (c), BUPERS Millington/NAVPERSCOM will provide their "fair share" of military personnel to augment the NAVSUPPACT Mid-South Security ASF.

4. Control Measures

a. Personnel Access

(1) Through the use of the CAC, the ACS provides personnel access control to NAVPERSCOM buildings and denies access to those not authorized. All personnel should wear their CAC on outer clothing and visible when away from their desks while inside NAVPERSCOM buildings.

(2) Per reference (a), a system of personnel identification is a required basic security measure. Positive identification provides a means for visually establishing authorization for personnel movement and actions. All personnel requiring access to NAVPERSCOM buildings are to be identified.

(3) All personnel accessing NAVPERSCOM buildings during FPCON DELTA are to check-in with the NAVPERSCOM Duty Office at the Jamie Whitten Building 791, room B-109, or by phone at 874-3071.

b. CAC

(1) When NAVPERSCOM buildings are secured the CAC is required for BUPERS Millington/NAVPERSCOM personnel (military, civilian, or government contract) to access buildings.

(2) Military, civilian, and contract personnel are issued their CAC at the Personnel Support Activity Detachment Mid-South, building 456. All BUPERS/Millington/NAVPERSCOM personnel must check-in and out of the command with NAVPERSCOM (PERS-534). Upon check-in, NAVPERSCOM (PERS-534) will provide required information to NAVSUPACT Mid-South Security to issue reporting personnel access required for their CAC. Questions concerning building access for NAVPERSCOM should be addressed to NAVPERSCOM (PERS-534) at 874-3082/3084/3088.

c. Visitors from Other Federal Agencies. Security representatives of the following agencies may be admitted to NAVPERSCOM buildings at any time upon presentation of their official agency credentials:

- (1) Federal Bureau of Investigation (FBI).
- (2) Military Intelligence (U.S. Army).
- (3) Naval Criminal Investigative Service (NAVCRIMINSERV).
- (4) Office of Special Investigations (U.S. Air Force).
- (5) Secret Service (Treasury Department).
- (6) Criminal Investigation Command (U.S. Army).
- (7) Defense Investigative Service (DIS).
- (8) Defense Criminal Investigative Service (DCIS).
- (9) Counterintelligence Credentials.

(10) U.S. Marshall's Service.

d. Level Two Restricted Access Areas. Visitor's requesting access to NAVPERSCOM spaces designated as "Level Two Restricted Access Areas" will be required to sign-in and out on an official visitor's log. NAVPERSCOM (PERS-534) will verify visiting personnel security clearance data prior to authorizing access to Level Two Restricted Access Areas. The following spaces are designated Level Two Restricted Access Areas.

(1) Ray Hall Building 453, room 327.

(2) Lt. Clyde Everett Lassen Building 457, room 294B.

(3) Goetsch Hall Building 768, rooms S107A and S305A.

(4) Wood Hall Building 769 room 184C and 184D.

(5) Jamie Whitten Building 791, rooms, B107A, D107B, F104, F204, and G101B.

5. Visit Requests. See reference (d) for information on visit requests.

6. Level I Awareness Training (AT)

a. NAVPERSCOM (PERS-534) will conduct Anti-terrorism/Force Protection (AT/FP) Level I training (individual AT awareness training) for all personnel (including family members of those on permanent change of station (PCS) orders) deploying or traveling Outside Continental United States (OCONUS), including Canada and Mexico.

b. Training will be conducted within 6 months prior to deployment or travel OCONUS.

c. When threat level rises above Low in the U.S., training will be provided to all BUPERS Millington/NAVPERSCOM personnel annually.

d. Level I training consist of the following:

(1) For OCONUS travel, a 45-minute briefing conducted by NAVPERSCOM (PERS-534) qualified Anti-terrorist Training Officer

24 AUG 2010

(ATTO) and viewing an anti-terrorism video is required. At the completion of this training, the individual(s) will receive the Joint Staff Guide 5260, Service Member's Personal Protection Guide, A Self-Help Handbook to Combating Terrorism, specific area update.

(2) For annual AT, personnel must either attend an all hands AT brief, attend training identified in paragraph (1) above or complete the AT Computer Based Training at <http://at-awareness.org> and forward the certificate of training completion to the ATTO for certification.

e. A Confirmation of Training Memorandum will be issued to each person to be used for a NAVPERS 1070/613 Administrative Remarks entry for military and a "Memorandum for the Record" for civilians.

f. A certification of training will be annotated in the remarks section of travel/leave orders, on country clearance requests, and in the NAVPERSCOM overseas screening message for PCS orders.

7. Material Control. The controlled movement of government owned property is important. This will be accomplished through the use of property passes and bills of lading. Incoming and outgoing deliveries/shipments will be coordinated through NAVPERSCOM (PERS-533).

8. Loss Prevention. Per reference (a), a loss prevention program is essential.

a. At BUPERS Millington/NAVPERSCOM the loss of government property will immediately be reported to:

(1) NAVPERSCOM, Inventory Management Section (PERS-533D) at 874-4007.

(2) NAVPERSCOM (PERS-534) at 874-3091.

(3) NAVSUPPACT Mid-South, NAVCRIMINSERV Office at 874-5387.

(4) NAVSUPPACT Mid-South Security Office at 874-5533/5534.

24 AUG 2010

b. NAVSUPPACT Mid-South Security will investigate all lost or stolen government property.

c. A DD 200 Financial Liability Investigation of Property Loss, will be used as the report to document the financial liability process for lost, damaged, or destroyed Government property. When completed, NAVPERSCOM (PERS-533D) will file the DD 200 as the official document for adjustment of property records. See reference (j), article 0140-200, Missing, Lost or Stolen Government-Owned Property, for guidance on completion of the DD 200.

9. Hazardous Material. Hazardous materials include, but are not limited to, the following categories: explosives, gases, flammable liquids, flammable solids, spontaneously combustible material, and material dangerous when wet, oxidizers and organic peroxides, poisonous and etiologic (infectious) materials, radioactive materials, corrosives, and miscellaneous hazardous materials. All hazardous materials at NAVSUPPACT Mid-South will be handled per reference (b).

10. Vehicle Control and Vehicle Registration. Per reference (b), NAVSUPPACT Mid-South Security is responsible for the vehicle control and registration program.

11. Key and Lock Control

a. NAVPERSCOM, Facilities/Space Management Section (PERS-533E) is designated as the command key custodian. Questions regarding the key and lock control program should be addressed directly to NAVPERSCOM (PERS-533E).

b. Offices, departments, or divisions shall designate a key control representative and an alternate in writing. Designations will be made via memorandum signed by department directors and forwarded to NAVPERSCOM (PERS-533). The designated key control representatives will act as the single point of contact for key control issues.

c. To obtain keys, each key control representative must forward a consolidated list (e-mail or memorandum) of required keys to NAVPERSCOM (PERS-533) via their department director or assistant. This list must identify:

- (1) Key control representative name and code;
- (2) Building name/number;
- (3) Door and room number for each key requested; and
- (4) Number of keys required for each door/room listed.

d. All transferring military/civilian employees of BUPERS Millington/NAVPERSCOM will be required to checkout with their office, department, or division key representative to facilitate key accountability.

12. Navy "Blue Dart" Terrorism Threat Warning Message

a. The Navy "Blue Dart" message is a means to disseminate an imminent terrorist threat warning to assets that are being targeted for terrorist attack. To qualify for a Navy "Blue Dart," the intelligence information must be credible, the terrorist threat must be directed against a specific Navy target, and the threat must contain a specific timeframe.

b. The Navy "Blue Dart" message will be disseminated by the Navy Antiterrorist Alert Center (NAVATAC) when specific and credible intelligence indicates that a terrorist attack is imminent.

c. The Navy "Blue Dart" message requires acknowledgement by immediate message from all action addressees to DIRNAVCRIMINSERV WASHINGTON DC//NAVATAC/24//, info CNO WASHINGTON DC//N312//. Additionally, the affected command should include their regular reporting chain of command in the information addressee section. The Navy "Blue Dart" does not take the place of existing reporting requirements. Any changes in the command's force protection status should be noted in the initial response. Follow-up messages are encouraged if additional force protection measures are implemented. When a Navy "Blue Dart" message is received, NAVSUPACT Mid-South will do the following:

- (1) Review on-scene force protection conditions and liberty policies in the threatened area. Any modifications or defensive actions taken should be addressed by immediate message, through the chain of command, to DIRNAVCRIMINSERV WASHINGTON DC//NAVATAC/24//, info CNO WASHINGTON DC//N312//.

(2) Protect threat warning information, to the maximum extent possible, consistent with the need to inform threatened commands in a timely fashion.

(3) Dissemination of the threat information is the responsibility of NAVSUPPACT Mid-South.

d. The primary means to communicate the threat warning will be via secure telephone where possible, unsecured if necessary.

e. Exercise Navy "Blue Dart" messages will be issued in support of CNO Integrated Vulnerability Assessments and specific major exercises on an ad hoc basis. Exercise Navy "Blue Dart" messages will assist the assessment teams and commanders in evaluating the information flow and force protection readiness of installations and units.

f. NAVATAC Navy "Blue Dart" messages will be addressed as follows:

(1) Action Addees. A "Blue Dart" will normally have only one action addree, the ship or unit that could be directly affected by a potential act of terrorism for which the NAVATAC has specific, imminent threat information. The only time a "Blue Dart" will have more than one action addree are:

(a) When multiple ships or units are affected; and

(b) When the specific unit threatened is a tenant command of a larger region or installation. All units that are in a position to directly affect the security posture of the impacted unit will be action addees.

(2) Information Addees. Typical information addees will include Fleet commanders, Regional commanders, Regional intelligence centers, and the local NAVCRIMINVSERV office.

13. Force Protection Condition (FPCON). Reference (k), chapter 10, describes the progressive level of protective measures implemented by all Department of Defense (DoD) components in response to terrorist threats. Terrorist threat levels are an intelligence community judgment about the likelihood of terrorist attack on DoD personnel and facilities. The FPCON is the principal means a commander has to implement an operational

decision regarding the protection of a military facility. Commanders at any level can establish FPCONs. A subordinate commander can establish a higher FPCON if local conditions or intelligence data warrant doing so. References (b) and (k) explain measures necessary to implement terrorist threat conditions pertinent to NAVSUPACT Mid-South and tenant commands. Enclosure (2) explains the terrorist FPCONs pertinent to NAVPERSCOM.

14. Crisis Management for Hostage Situations, Terrorist Attacks, Barricaded Persons, Civil Disturbance, Major Accidents, Sabotage, Explosions, and Natural Disasters. When any of these crisis situations occur, NAVPERSCOM Command Duty Officer will be notified; however, NAVSUPACT Mid-South will assume command of any activity relating to these crisis management situations at NAVSUPACT Mid-South.

FORCE PROTECTION CONDITIONS (FPCON)

1. Information. The measures below describe the progressive response to a terrorist threat to Department of the Navy (DON) facilities and personnel. These are common security measures designed to facilitate inter-service coordination and support U.S. military anti-terrorism activities. Reference (b) provides the steps that will be taken by NAVSUPACT Mid-South in setting FPCON.

2. Purpose. The purpose of the FPCON system is accessibility to, and easy dissemination of appropriate information. The declaration, reduction, and cancellation of FPCONs remain the exclusive responsibility of the commanders specified.

3. FPCON

a. FPCON NORMAL. FPCON NORMAL applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.

(1) Measure NORMAL 1. Secure and randomly inspect buildings, rooms, and storage areas not in regular use. (See appendix A).

(2) Measure NORMAL 2. Conduct random security spot checks of vehicles and persons entering facilities under the jurisdiction of the United States.

(3) Measure NORMAL 3. Limit access points for vehicles and personnel commensurate with reasonable flow of traffic.

b. FPCON ALPHA Measures. FPCON ALPHA applies when there is a general threat of possible terrorist activity against personnel or facilities, the nature and extent of which are unpredictable. ALPHA measures must be capable of being maintained indefinitely.

(1) Measure ALPHA 1. Continue, or introduce, all measures in previous FPCON.

(2) Measure ALPHA 2. At regular intervals, inform personnel and family members of the general situation. Ensure personnel arriving for duty are briefed on the threat. Also,

24 AUG 2010

remind them to be alert for and report suspicious activities, such as the presence of unfamiliar personnel and vehicles, suspicious parcels, and possible surveillance attempts.

(3) Measure ALPHA 3. The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Plans should be in place to execute access control procedures. Key personnel required to implement security plans should be on-call and readily available. (See appendix B).

(4) Measure ALPHA 4. Increase security spot checks of vehicles and persons entering installations under the jurisdiction of the United States.

(5) Measure ALPHA 5. Initiate food and water operational risk management procedures, brief personnel on food and water security procedures, and report any unusual activities.

(6) Measure ALPHA 6. Test mass notification system.

(7) Measure ALPHA 7. Review all plans, identify resource requirements, and be prepared to implement higher FPCONs.

(8) Measure ALPHA 8. Review and, if necessary, implement security measures for high-risk personnel.

(9) Measure ALPHA 9. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

(10) Measure ALPHA 10. Review intelligence, counter intelligence, and operations dissemination procedures.

c. FPCON BRAVO Measures. FPCON BRAVO applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and relations with local authorities.

(1) Measure BRAVO 1. Continue, or introduce, all measures in previous FPCONs. (See appendix C).

24 AUG 2010

(2) Measure BRAVO 2. Enforce control of entry onto U.S. infrastructures critical to mission accomplishment, lucrative targets, and high profile locations; and randomly search vehicles entering the areas. Particular scrutiny should be given to vehicles that are capable of concealing a large improvised explosive device (IED) (cargo vans, delivery vehicles) sufficient to cause catastrophic damage or loss of life.

(3) Measure BRAVO 3. Identify critical and high occupancy buildings. Keep cars and objects (e.g., crates, trash containers) away from buildings to reduce vulnerability to bomb attacks. Apply this criterion to all inhabited structures to the greatest extent possible. Standoff distance should be determined by the following factors: asset criticality; the protection level provided by structure, IED/vehicle borne IED threat; and available security measures. Consider centralized parking.

(4) Measure BRAVO 4. Secure and inspect all buildings, rooms and storage areas not in regular use. (See appendix A)

(5) Measure BRAVO 5. At the beginning and end of each workday, as well as at random intervals, inspect the interior and exterior of buildings in regular use for suspicious packages. (See annex D)

(6) Measure BRAVO 6. Implement mail-screening procedures to identify suspicious letters and parcels.

(7) Measure BRAVO 7. Randomly inspect commercial deliveries. Advise family members to check home deliveries.

(8) Measure BRAVO 8. Randomly inspect food and water for evidence of tampering/contamination before use by DoD personnel. Inspections should include delivery vehicles and storage area/containers.

(9) Measure BRAVO 9. Increase security/guard presence or patrol/surveillance of DoD housing areas, schools, messes, on-base clubs, and similar high occupancy targets to improve deterrence and defense, and to build confidence among staff and family members.

24 AUG 2010

(10) Measure BRAVO 10. Implement plans to enhance off-installation security of DoD facilities. In areas with Threat Levels of Moderate, Significant, or High, coverage includes facilities (e.g., DoD schools and daycare centers) and transportation services and routes (e.g., bus routes) used by DoD employees and family members.

(11) Measure BRAVO 11. Inform local security committees of actions being taken.

(12) Measure BRAVO 12. Verify identity of visitors and randomly inspect their suitcases, parcels, and other containers.

(13) Measure BRAVO 13. Conduct random patrols to check vehicles, personnel, and buildings.

(14) Measure BRAVO 14. As necessary, implement additional security measures for high-risk personnel.

(15) Measure BRAVO 15. Place personnel required for implementing antiterrorism plans on call; commanders should exercise discretion in approving absences.

(16) Measure BRAVO 16. Identify and brief personnel who may augment guard forces. Review specific rules of engagement including the use of deadly force.

(17) Measure BRAVO 17. As deemed appropriate, verify identity of personnel entering buildings.

(18) Measure BRAVO 18. Review status and adjust as appropriate operations security, communications security, and information systems security procedures.

(19) Measure BRAVO 19 (airfield specific). As appropriate, erect barriers and man and establish checkpoints at entrances to airfields. Ensure identity of all individuals entering the airfield (flightline and support facilities) - no exceptions. Randomly inspect vehicles, briefcases, and packages entering the airfield.

(20) Measure BRAVO 20 (airfield specific). Coordinate plans to safeguard aircraft departure and approach flight paths with local authorities. Be prepared to activate contingency

24 AUG 2010

plans and issue detailed air traffic control procedures. As appropriate, take actions to mitigate threat of surface-to-air missiles or standoff weapons that can be delivered from beyond the airfield perimeter.

d. FPCON CHARLIE Measures. FPCON CHARLIE applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of CHARLIE measures may create hardship and affect the activities of the unit and its personnel.

(1) Measure CHARLIE 1. Continue, or introduce, all measures in previous FPCON. (See appendix C)

(2) Measure CHARLIE 2. Recall additional required personnel. Ensure armed augmentation security personnel are aware of current rules of engagement and Status of Forces Agreements. Review types of weapons and ammunition issued to augmentation security personnel; heightened threats may require employment of different weapon capabilities.

(3) Measure CHARLIE 3. Be prepared to react to requests for assistance, from both local authorities and other installations in the region.

(4) Measure CHARLIE 4. Limit access points to strictly enforce entry. Randomly search vehicles. (See appendix B)

(5) Measure CHARLIE 5. Ensure or verify identity of all individuals entering food and water storage and distribution centers, use sign in/out logs at access control/entry points, and limit/inspect all personal items.

(6) Measure CHARLIE 6. Initiate contingency monitoring for biological and chemical agents as required. Suspend contractors/off-facility users from tapping into facility water system (alternate locally developed measure should be executed when contractors are responsible for DoD water supplies or when water is provided by local (non-DoD) sources or agencies).

(7) Measure CHARLIE 7. Increase standoff from sensitive buildings based on threat. Implement barrier plan to hinder vehicle borne attack.

(8) Measure CHARLIE 8. Increase patrolling of the facility to include waterside perimeters, if appropriate. Be prepared to assist local authorities in searching for threatening actions/persons outside the facility perimeter. For airfields, patrol or provide observation of approach and departure flight corridors as appropriate to the threat (coordinate with Transportation Security Administration (TSA), Marine Patrol, U.S. Coast Guard, and local law enforcements as required to cover off-facility approach and departure flight corridors).

(9) Measure CHARLIE 9. Protect all designated infrastructure critical to mission accomplishment. Give special attention to and coordinate with local authorities regarding infrastructure outside the military establishment.

(10) Measure CHARLIE 10. To reduce vulnerability to attack, consult local authorities about closing public (and military) roads and facilities and coordinate any other precautionary measures taken outside the installation perimeter.

(11) Measure CHARLIE 11. Consider searching suitcases, briefcases, packages, etc., being brought onto the installation through access control points and consider randomly searching suitcases, briefcases, packages, etc., leaving.

(12) Measure CHARLIE 12. Review personnel policy procedures to determine course of action for family members.

(13) Measure CHARLIE 13. Review access procedures for all non-U.S. personnel and adjust as appropriate. For airfields, consider terminating visitor access to the flightline and support facilities.

(14) Measure CHARLIE 14. Consider escorting children to and from DoD schools (among options to consider are escorting school buses, recommending parents escort children to/from school, etc.)

(15) Measure CHARLIE 15 (airfield specific). Reduce flying to essential operational flights only. Implement appropriate flying countermeasures as directed by the flight wing commander (military aircraft) or TSA (civilian aircraft).

24 AUG 2010

Consider relief landing ground actions to take aircraft diversions into and out of an attacked airfield. Consider augmenting fire-fighting details.

e. FPCON DELTA Measures. FPCON DELTA applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specified 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.

- (1) Measure DELTA 1. Continue, or introduce, all measures in previous FPCON. (See appendix C)
- (2) Measure DELTA 2. Augment guards as necessary.
- (3) Measure DELTA 3. Identify all vehicles within operational or mission support areas.
- (4) Measure DELTA 4. Search all vehicles and their contents before allowing entrance to the installation.
- (5) Measure DELTA 5. Control facility access and implement positive identification of all personnel - NO EXCEPTIONS.
- (6) Measure DELTA 6. Search all suitcases, briefcases, packages, etc., brought onto the installation.
- (7) Measure DELTA 7. Close DoD schools and/or escort children to/from DoD schools as required.
- (8) Measure DELTA 8. Make frequent checks of the exterior of buildings and of parking areas.
- (9) Measure DELTA 9. Restrict all non-essential movement.
- (10) Measure DELTA 10 (airfield specific). Cease all flying except for specifically authorized operational sorties. Be prepared to deploy light aircraft/helicopters for surveillance tasks or to move internal security forces. Implement, if necessary, appropriate flying countermeasures.

(11) Measure DELTA 11 (airfield specific). As appropriate, airfields should prepare to accept aircraft diverted from other stations.

(12) Measure DELTA 12. If permitted, close public and military roads and facilities. If applicable, close military roads allowing access to the airfield.

24 AUG 2010

APPENDIX A

1. NAVPERSCOM (PERS-533) will conduct daily building checks to ensure secure rooms, storage areas, and spaces not in use are locked and report completion of all security checks and results to the NAVPERSCOM Duty Office.
2. Report all suspicious packages or personnel to NAVSUPACT Mid-South Security at 874-5533/5534.
3. A building security checklist (appendix D) is provided for each NAVPERSCOM building.

APPENDIX B

FPCON MEASURE ALPHA 3 LIST OF KEY PERSONNEL

1. NAVPERSCOM (PERS-53) shall take action to notify the personnel listed of the current FPCON and ensure personnel are readily available.

FPCON KEY PERSONNEL

NAVPERSCOM (PERS-53)	Director, Command Support Services Division
NAVPERSCOM (PERS-534)	Head Security
NAVPERSCOM (PERS-533)	Head, Integrated Logistics Branch
NAVPERSCOM (PERS-533E)	Head, Facilities/Space Management
NAVPERSCOM (PERS-codes)	ASF Personnel

APPENDIX C

ESTABLISH FPCON BUILDING SECURITY/ROVING PATROL WATCH BILL

1. The responsible PERS-code for each building will establish a FPCON building security/roving patrol watch bill at the setting of FPCON BRAVO to be implemented upon setting FPCON CHARLIE. The senior watch officer (SWO) can assist in providing names of military personnel available for the security/roving watch. The building security and roving watch will be set when personnel are present in the building. Training for personnel standing the security watch and roving patrol watch is coordinated through NAVPERSCOM (PERS-534) at 874-3089. NAVPERSCOM departments shall provide a listing of "Essential Personnel" requiring installation "Drive On" or "Shuttle" privilege to NAVPERSCOM (PERS-534) in preparation for the possibility of setting FPCON DELTA. NAVPERSCOM (PERS-534) will ensure all NAVPERSCOM building entries are locked upon setting FPCON CHARLIE. Below are the responsible organization/ PERS-code for each NAVPERSCOM building.

NAVPERSCOM BUILDING	RESPONSIBLE ORGANIZATION/PERS-CODE
Ray Hall, Bldg 453	BUPERS (BUPERS-3)
LT Clyde Everett Lassen Building, Bldg 457	OPNAV N135
Goetsch Hall, Bldg 768	NAVPERSCOM (PERS-9)
Wood Hall, Bldg 769	NAVPERSCOM (PERS-3)
LT Vincent R. Capodanno Building, Bldg 785	BUPERS (BUPERS-1)
CAPT John Philip Cromwell Building, Bldg 789	NAVPERSCOM (PERS-5)
Jamie Whitten Building, Bldg 791	NAVPERSCOM (PERS-4)

2. Upon setting of FPCON CHARLIE, the FPCON building security/roving patrol watch bill will be set. The designated entry and exit door at each NAVPERSCOM building is as follows to limit access to NAVPERSCOM buildings.

BUILDING	DOOR
Ray Hall, Bldg 453	Main Entrance
LT Clyde Everett Lassen Building, Bldg 457	South Center Connector Door
Goetsch Hall, Bldg 768	Southeast Entrance
Wood Hall, Bldg 769	Selection Board Entrance
LT Vincent R. Capodanno Building, Bldg 785	East Entrance
CAPT John Philip Cromwell Building, Bldg 789	West Entrance
Jamie Whitten Building, Bldg 791	South (Main) Entrance

3. Building entrance points will be manned during building hours of operation.

4. Controlled access and positive identification of all personnel entering building is required. **NO EXCEPTIONS.**

a. The building security watch personnel will:

- (1) Stand a 4-hour watch at the designated entrance;
- (2) Be a military Service member or government civilian;
- (3) Check identification;
- (4) Search all items;
- (5) Require all personnel to sign-in/out of the building each time they enter or depart;
- (6) Maintain a security watch log; and

24 AUG 2010

(7) Report immediately to the responsible building PERS-code or designated representative any circumstances that are considered a security risk or threat.

b. The building security roving patrol watch will:

(1) Report to the building security watch when assuming the watch;

(2) Stand a 4-hour watch;

(3) Act as assistant building security watch when not making building rounds; and

(4) Make rounds of the building every hour on the hour and report to the building security watch when security rounds are completed.

c. Personnel assigned FPCON DELTA watches shall perform security checks (see appendix D) and:

(1) Ensure vacant office spaces, electrical, data and telephone closets, and roof accesses are locked;

(2) Ensure all loading dock and exterior machinery room doors are locked;

(3) Report all unlocked spaces and any circumstances that are considered a security risk or threat to the building security watch.

d. A cell phone will be made available to the building security and roving patrol watch personnel when assuming the watch.

e. Upon setting of FPCON DELTA, all spaces not occupied must be secured. It is the responsibility of the last person vacating an office space to turn-off all lights, secure coffeepots, etc., and lock the office space.

f. All personnel will be required to wear their CAC when away from their desks in such a manner that the card is visible.

24 AUG 2010

g. If FPCON DELTA is set during the workday, departments will be directed to start securing all "non-essential" personnel. Personnel will be secured at intervals to prevent traffic back up at the gates. When securing "non-essential" personnel, departments will advise individuals to listen to local radio/television or call 874-4968 each day for information concerning the recall to duty/work. Lassen Building 457 will dismiss their personnel first followed, by Ray Hall Building 453, Goetsch Hall Building 768, Capodanno Building 785, Wood Hall Building 769, Cromwell Building 789, and Whitten Building 791.

h. All personnel will be advised when FPCON DELTA is set. After normal working hours an announcement on the local radio/television will be made stating the base is closed and only "Essential Personnel" are to report for duty/work.

i. The following only applies to Capodanno Building 785: If FPCON DELTA is set, the requirement for a security watch/roving patrol is negated.

5. Each building security watch stander will be briefed on specific responsibilities by the CDO or the current NPC watch officer prior to manning entry points.

APPENDIX D

**LT CLYDE EVERETT LASSEN BUILDING, BLDG 457
SECURITY CHECKLIST CNO (N135)/CNIC DET**

Check the following areas. Any suspicious activity or condition should be immediately reported by phone to NAVSUPACT Mid-South Security at 874-5533/5534 and NAVPERSCOM Security Manager (PERS-534) at 874-3091. Upon completion of security checks, the checklist will be retained in the NAVPERSCOM Duty Office.

PERIMETERS ROOMS	PERIMETER DOORS	LOCKED	UNLOCKED	REMARKS
MECHANICAL ROOM 103 SOUTH SIDE	ENTRY DOOR			
LOADING DOCK AREA WEST SIDE	ROLL-UP DOORS			LOCKED WHEN NOT IN USE.
MECHANICAL ROOM 020 NORTH SIDE	ENTRY DOOR			
MAIL ROOM 007 NORTH SIDE	ENTRY DOOR			
MECHANICAL ROOM 078 EAST SIDE	ENTRY DOOR			
TELEPHONE SWITCH ROOM 028 EAST SIDE	ENTRY DOOR			

INTERNAL ROOM NO.	SPACES	LOCKED	UNLOCKED	REMARKS
004	PRINT SHOP			LOCKED WHEN NOT IN USE.
006	MAIL ROOM			LOCKED WHEN NOT IN USE.
008	STORAGE			LOCKED WHEN NOT IN USE.
013	OFFICE/STORAGE			
019	ELECTRICAL CLOSET			
025	ELECTRICAL CLOSET			
026	TELEPHONE CLOSET			
027	LAN DATA CLOSET			
028	TELEPHONE SWITCH			

INTERNAL ROOM NO.	SPACES	LOCKED	UNLOCKED	REMARKS
030	STORAGE (OPPOSITE ROOM 031)			
034	JANITORIAL CLOSET			LOCKED WHEN NOT IN USE.
070	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
073	JANITORIAL CLOSET			LOCKED WHEN NOT IN USE.
055	ELECTRICAL CLOSET FIRST FLOOR AT ELEVATOR ON SOUTH SIDE			
054	ELEVATOR MAINTENANCE ROOM FIRST FLOOR SOUTH SIDE			
049	ELEVATOR MAINTENANCE ROOM FIRST FLOOR NORTH SIDE			
076	STORAGE			
077	OFFICE			LOCKED WHEN NOT IN USE.
078	MECHANICAL ROOM			
081	STORAGE			
083	ELECTRICAL CLOSET			
085	TELEPHONE CLOSET			
086	LAN DATA CLOSET			
094/095	OFFICE/STORAGE			LOCKED WHEN NOT IN USE.
097	OFFICE			LOCKED WHEN NOT IN USE
098	STORAGE			
100	PROJECTOR ROOM			
101	TRAINING ROOM			LOCKED WHEN NOT IN USE.
103A	MECHANICAL ROOM			
111	STORAGE			LOCKED WHEN NOT IN USE.

INTERNAL ROOM NO.	SPACES	LOCKED	UNLOCKED	REMARKS
112	VIDEO INSPECTION			LOCKED WHEN NOT IN USE
115	STORAGE			
117	STORAGE			
216	STORAGE			
220	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
222	ELECTRICAL CLOSET			
224	MECHANICAL ROOM			
229	ELECTRICAL CLOSET			
230	TELEPHONE CLOSET			
231	LAN DATA CLOSET			
232	BREAK ROOM STORAGE			
235	JANITORIAL CLOSET			
239/240	CONFERENCE & STORAGE ROOM			LOCKED WHEN NOT IN USE.
247	ELEVATOR MAINTENANCE CLOSET			
259/260	CONFERENCE & STORAGE ROOM			LOCKED WHEN NOT IN USE.
263	JANITORIAL CLOSET			
268	STORAGE			
270	ELECTRICAL CLOSET			
277	ELECTRICAL CLOSET			
278	TELEPHONE CLOSET			
279	LAN DATA CLOSET			
283	STORAGE			
289	LIBRARY/CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
294B	SIPRNET ROOM			
294C	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
305	RESOUCE LIBRARY			LOCKED WHEN NOT IN USE.

INTERNAL ROOM NO.	SPACES	LOCKED	UNLOCKED	REMARKS
309	STORAGE			
314	ELECTRICAL CLOSET			
316	MECHANICAL ROOM			
320	ELECTRICAL CLOSET			
321	TELEPHONE CLOSET			
322	LAN DATA CLOSET			
326	JANITORIAL CLOSET			
344	ELEVATOR MAINTENANCE ROOM			
353	CLASS ROOM			LOCKED WHEN NOT IN USE.
357	JANITORIAL CLOSET			
360	CLASS ROOM			LOCKED WHEN NOT IN USE.
361	CLASS ROOM			LOCKED WHEN NOT IN USE.
362	ELECTRICAL CLOSET			
370	ELECTRICAL CLOSET			
371	TELEPHONE CLOSET			
372	LAN DATA CLOSET			
373	BREAK ROOM STORAGE			
374	STORAGE			
386	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
390	STORAGE			
396	MEDIA RESOURCE CENTER			LOCKED WHEN NOT IN USE.
397	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
	NORTH SIDE STAIRWELL ACCESS DOORS TO ROOF			
	SOUTH SIDE STAIRWELL ACCESS DOORS TO ROOF			

APPENDIX D

GOETSCH HALL, BLDG 768
 SECURITY CHECK LIST (PERS-9)

Check the following areas. Any suspicious activity or condition should be immediately reported by phone to NAVSUPACT Mid-South Security at 874-5533/5534 and the NAVPERSCOM Security Manager (PERS-534) at 874-3091. Upon completion of security check, the checklist will be retained in the NAVPERSCOM Duty Office.

INTERNAL ROOM NR.	SPACES	LOCKED	UNLOCKED	REMARKS
EL-101	ELEVATOR MAINTENANCE CLOSET			
E-103	TELEPHONE CLOSET			
E-105	LAN DATA CLOSET			
N-103	STORAGE CLOSET			
N-105	ELECTRICAL CLOSET			
N-106A	TELEPHONE CLOSET			
N-106B	LAN DATA CLOSET			
N-107	MAIL ROOM			
N-109	NURSING ROOM			
N-110	STORAGE			
N-111	ELECTRICAL CLOSET			
W-104	LAN DATA CLOSET			
W-106	TELEPHONE CLOSET			
S-102	SUPPLY STORAGE			
S-103	STORAGE			
S-104	ELECTRICAL CLOSET			
S-107A	SIPRNET ROOM			
S-108	JANITORIAL CLOSET			
S-110	ELECTRICAL CLOSET			
S-112	MECHANICAL CLOSET			
EL-201	ELEVATOR MAINTENANCE CLOSET			
S-201A	STORAGE			
S-201B	STORAGE			
S-201C	VTC ROOM			
E-203	TELEPHONE CLOSET			
E-205	LAN DATA CLOSET			
N-203	STORAGE			

INTERNAL ROOM NO.	SPACES	LOCKED	UNLOCKED	REMARKS
N-205	ELECTRICAL CLOSET			
N-211	FACILITY STORAGE			
N-213	ELECTRICAL CLOSET			
N-215	TELEPHONE SUPPLY STORAGE			
W-204	LAN DATA CLOSET			
W-206	TELEPHONE CLOSET			
S-204	ELECTRICAL CLOSET			
S-208	JANITORIAL CLOSET			
S-210	ELECTRICAL CLOSET			
S-212	MECHANICAL ROOM			
EL-301	ROOF ACCESS			
EL-302	ELEVATOR MAINTENANCE CLOSET			
E-303	TELEPHONE CLOSET			
E-305	LAN DATA CLOSET			
N-303	STORAGE			
N-305	ELECTRICAL CLOSET			
N-307	FACILITY STORAGE			
N-309	STORAGE			
N-311	STORAGE			
N-312	FACILITY STORAGE			
N-313	ELECTRICAL CLOSET			
N-315	STORAGE CLOSET			
W-303	LAN DATA CLOSET			
W-305	TELEPHONE CLOSET			
S-304	ELECTRICAL CLOSET			
S-306	BOILER ROOM			
S-308	MECHANICAL ROOM			
S-310	ELECTRICAL CLOSET			
S-312	STORAGE			

APPENDIX D

**WOOD HALL, BLDG 769
SECURITY CHECKLIST (PERS-3)**

Check the following areas. Any suspicious activity or condition should be immediately reported by phone to NAVSUPACT Mid-South Security at 874-5533/5534 and the NAVPERSCOM Security Manager (PERS-534) at 874-3091. Upon completion of security check, the checklist will be retained in the NAVPERSCOM Duty Office.

PERIMETER ROOMS	PERIMETER DOORS	LOCKED	UNLOCKED	REMARKS
LOADING DOCK	ROLL-UP DOOR			
GENERATOR SOUTH SIDE	EMERGENCY POWER			
TOWER SOUTH SIDE	COOLING TOWER			
MECHANICAL ROOM SOUTH SIDE	ENTRY DOORS			
UTILITY ENTRY EAST SIDE	ENTRY DOOR			

INTERNAL ROOM NR.	SPACES	LOCKED	UNLOCKED	REMARKS
184/185	SECURITY SPACES			LOCKED WHEN NOT IN USE
181	CLOSET			
180	CLOSET			
178	MAINTENANCE ROOM			
178 A, B, C	LAN DATA CLOSET TELEPHONE CLOSET ELECTRICAL CLOSET			
186	RECORD STORAGE			
143	MECHANICAL ROOM			
108	MAINTENANCE ROOM			
108 A, B, C	LAN DATA CLOSET TELEPHONE CLOSET ELECTRICAL CLOSET			
106A	JANITORIAL CLOSET			
111	TELEPHONE CLOSET			
162	LAN DATA CLOSET			
163	ELECTRICAL CLOSET			
148B	KEY ROOM			
148	MECHANICAL ROOM			

INTERNAL ROOM NR.	SPACES	LOCKED	UNLOCKED	REMARKS
148 C, D	LAN DATA CLOSET TELEPHONE CLOSET			
154	NURSING ROOM			
151	ELECTRICAL/STORAGE ROOM IN CAFETERIA			
157C	SUPPLY ROOM			
158C	SUPPLY ROOM			
160	STORAGE ROOM			
164	ELECTRICIAL CLOSET			
165	JANITORIAL CLOSET			
168	HOT WATER TANK CLOSET			
173	LOADING DOCK AREA			
174	MAIL ROOM			
176	MECHANICAL ROOM			
145	A&B CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
161	VTC CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
182	JANITORIAL CLOSET			
103	ALL PURPOSE HOLDING ROOM			
112	SELECTION BOARD			SELECTION BOARD SPACES LOCKED WHEN NOT IN USE
128	SPONSOR/TECHNICAL ADVISOR ROOM			
130A	CUSTODIAL CLOSET			
131A	VALVE ROOM			
132A	FIRE SPRINKLER EQUIPMENT ROOM			
195	EMPRS OPERATIONS			

APPENDIX D

LT VINCENT R. CAPODANNO BUILDING, BLDG 785
 SECURITY CHECK LIST BUPERS (BUPERS-1)

Check the following areas. Any suspicious activity or condition should be immediately reported by phone to NAVSUPACT Mid-South Security at 874-5533/5534 and the NAVPERSCOM Security Manager (PERS-534) at 874-3091. Upon completion of security check, the checklist will be retained in the NAVPERSCOM Duty Office.

BUILDING PERIMETER	PERIMETER OF BUILDING	LOCKED	UNLOCKED	REMARKS
EAST SIDE OF BUILDING	ROLL-UP DOOR			CLOSED WHEN NOT IN USE.

INTERNAL ROOM NR.	SPACES	LOCKED	UNLOCKED	REMARKS
101	NAVY SOCIAL SCIENCE EXPERIMENTAL LABORATORY			LOCKED WHEN NOT IN USE.
105	BUSINESS PROCESS REENGINEERING LABORATORY			LOCKED WHEN NOT IN USE.
113	WORKFORCE MANAGEMENT LABORATORY			LOCKED WHEN NOT IN USE.
114	SURVEY OPERATIONS			
116	EXERCISE ROOM			
118	SURVEY OPERATIONS			LOCKED WHEN NOT IN USE.
123	TECHNICAL WRITER/IRB ADMINISTRATOR			
127	ELECTRICAL/JANITORIAL CLOSET			
130	RMO STORAGE			
132	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
134	ELECTRICAL/JANITORIAL CLOSET			
137	LAN DATA CLOSET			
138	TELEPHONE CLOSET			
142	MECHANICAL ROOM			
143	TELEPHONE CLOSET			
144	LAN DATA CLOSET			

BUILDING PERIMETER	PERIMETER OF BUILDING	LOCKED	UNLOCKED	REMARKS
--------------------	-----------------------	--------	----------	---------

157	LIMITED ACCESS REPORTS			
171A	STORAGE CLOSET			

INTERNAL ROOM NR.	SPACES	LOCKED	UNLOCKED	REMARKS
245	ELECTRICAL CLOSET			
250	STORAGE CLOSET			
251	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
253	LAN DATA CLOSET			
254	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
255	LAN DATA CLOSET			
256	TELEPHONE CLOSET			
262	MECHANICAL ROOM			
263	COMPUTER ROOM			LOCKED WHEN NOT IN USE.
266	WAREHOUSE			LOCKED WHEN NOT IN USE.
266A	WAREHOUSE STORAGE CAGE			LOCKED WHEN NOT IN USE.
267	MECHANICAL ROOM			
268	JANITORIAL CLOSET			
269	CHILLER ROOM			

APPENDIX D

**CAPT JOHN PHILIP CROMWELL BUILDING, BLDG 789
 SECURITY CHECK LIST (PERS-3)**

Check the following areas. Any suspicious activity or condition should be immediately reported by phone to NAVSUPACT Mid-South Security at 874-5533/5534 and the NAVPERSCOM Security Manager (PERS-534) at 874-3091. Upon completion of security check the checklist will be retained in the NAVPERSCOM Duty Office.

BUILDING PERIMETER	PERIMETER OF BUILDING	LOCKED	UNLOCKED	REMARKS
ENTRY DOOR	SOUTH SIDE MECHANICAL ROOM			
ENTRY DOOR	WEST SIDE UPS ROOM			
AIR HANDLER AREA	WEST SIDE			
AIR HANDLER AREA	SOUTH SIDE			

INTERNAL ROOM NR.	SPACES	LOCKED	UNLOCKED	REMARKS
113	TELEPHONE CLOSET			
114	JANITORIAL CLOSET			
110	STORAGE ROOM			
120	LAN DATA CLOSET			
115	PRINT ROOM			
104	WAN ROOM			

APPENDIX D

JAMIE WHITTEN BUILDING, BLDG 791
 SECURITY CHECK LIST (PERS-4)

Check the following areas. Any suspicious activity or condition should be immediately reported by phone to NAVSUPACT Mid-South Security at 874-5533/5534 and the NAVPERSCOM Security Manager (PERS-534) at 874-3091. Upon completion of security check the checklist will be retained in the NAVPERSCOM Duty Office.

BUILDING PERIMETER	PERIMETER OF BUILDING	LOCKED	UNLOCKED	REMARKS
SOUTH SIDE OF BUILDING	ROLL-UP DOOR AND SUPPLY ROOM			
NORTH EAST SIDE BUILDING	AIR HANDLING EQUIPMENT ROOM			
INTERNAL ROOM NR.	SPACES	LOCKED	UNLOCKED	REMARKS
B103B	TELEPHONE CLOSET			
B103C	LAN DATA CLOSET			
B108	MECHANICAL ROOM			
B111/113	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
B117A	LAN DATA CLOSET			
B117B	TELEPHONE CLOSET			
B109	DUTY OFFICE			
B107A	SIPRNET SPACE			
B118	MECHANICAL ROOM			
F106	STORAGE CLOSET			
F103/F104	SIPRNET SPACE			
F107	STORAGE ROOM/CLOSET			
F113	LAN DATA CLOSET			
F115	TELEPHONE CLOSET			
F117	ELECTRICAL CLOSET			
D107B	SIPRNET SPACE			
D109	MECHANICAL ROOM			
D101	MECHANICAL ROOM			
E101E	MECHANICAL ROOM			
C101	STORAGE CLOSET			

24 AUG 2010

INTERNAL ROOM NR.	SPACES	LOCKED	UNLOCKED	REMARKS
H101E	MECH/DATA/TELE			
G109	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
G111	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
G114	ELECTRICAL CLOSET			
G112	TELEPHONE CLOSET			
G110	LAN DATA CLOSET			
C108	ELEVATOR CONTROL			
C110	STORAGE CLOSET			
G202	LAN DATA CLOSET			
G204	TELEPHONE CLOSET			
G206	ELECTRICAL CLOSET			
G201	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
G205	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
F206	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
F202	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
F201	LAN DATA CLOSET			
F203	TELEPHONE CLOSET			
F205	ELECTRICAL CLOSET			
C208	STORAGE CLOSET			
C206	STORAGE CLOSET			
STAIR WELL	ROOF ACCESS			

APPENDIX D

**RAY HALL BUILDING, BLDG 453
 SECURITY CHECK LIST (BUPERS-3)**

Check the following areas. Any suspicious activity or condition should be immediately reported by phone to NAVSUPACT Mid-South Security at 874-5533/5534 and the NAVPERSCOM Security Manager (PERS-534) at 874-3091. Upon completion of security check the checklist will be retained in the NAVPERSCOM Duty Office.

BUILDING PERIMETER	PERIMETER OF BUILDING	LOCKED	UNLOCKED	REMARKS
EAST SIDE OF BUILDING	OUTER MECHANICAL/ELECTRICAL ROOM			
NORTH EAST SIDE OF BUILDING	ROLL-UP DOOR AND WALK THROUGH WAREHOUSE DOOR			
NORTH CENTRAL SIDE OF BUILDING	ELECTRICAL CLOSET			
INTERNAL ROOM NR.	SPACES	LOCKED	UNLOCKED	REMARKS
101	STORAGE			
108	MAILROOM			
109	DATA/TELEPHONE CLOSET			
116	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
119	JANITOR CLOSET			
130 (INNER DOOR)	ELECTRICAL CLOSET			
139	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
201	STORAGE			
204	IG CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
211	MECHANICAL ROOM			
212	ELECTRICAL CLOSET			
213	ELEVATOR CLOSET			
215	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
216	JANITOR CLOSET			

NAVPERSCOMINST 5530.1E
24 AUG 2010

INTERNAL ROOM NR.	SPACES	LOCKED	UNLOCKED	REMARKS
229 (INNER DOOR)	ELECTRICAL CLOSET			
301	STORAGE			
308	DATA/TELEPHONE CLOSET			
313	MECHANICAL ROOM			
315	ELECTRICAL ROOM			
317	CONFERENCE ROOM			LOCKED WHEN NOT IN USE.
318	JANITOR CLOSET			
327	SIPRNET			
334	ELECTRICAL CLOSET			