

DEPARTMENT OF THE ARMY
U.S. Army Corps of Engineers
Humphreys Engineer Center
Alexandria, VA 22315-3860

HECR 380-1-2

CEHEC-SH

HEC Regulation
No. 380-1-2

1 March 2001

Security
HEC PHYSICAL SECURITY PLAN

1. Purpose. To implement internal security measures and controls within the Humphreys Engineer Center (HEC). The intent is to protect personnel as well as government and personal property.
2. Applicability. This regulation applies to all activities, organizational elements, tenants, and visitors at the Humphreys Engineer Center.
3. Distribution Statement. Approved for public release: distribution is unlimited.
4. References:
 - a. 190-11, Physical Security of Arms, Ammunition, and Explosives.
 - b. AR 190-13, The Army Physical Security Program.
 - c. AR 190-16, Physical Security.
 - d. AR 190-51, Security of Unclassified Army Property (Sensitive and Nonsensitive).
 - e. AR 380-4, DA Physical Security Program in the National Capital Region.
 - f. AR 380-5, DA Information Security Program.
 - g. AR 380-19, Information Systems Security.
 - h. DoD 2000.12, DoD Anti Terrorism/Force Protection (AT/FP) Program.
 - i. DoD 0-2000.12H, Protection of DoD Personnel and Activities Against Act of Terrorism and Political Turbulence.

This regulation supersedes Memorandum, 30 October 1992, and HECSA Physical Security Plan, 9 September 1999.

1 Mar 01

j. AR 525-13, 26 June 1992, DOD 2000.12, 15 September 1996, DOD 2000.12H, February 1993, JP 3-07.2, 17 March 1998, Threatcon Measures.

5. Responsibilities.

a. The Director of HECSA is responsible for providing normal protection for the buildings, its occupants, and government and private property.

b. The HECSA Security Manager is responsible for planning, formulating, and coordinating the overall physical security plan.

c. The Commander or Director of each activity is responsible for the security within their respective areas.

d. All employees are responsible for General Area Security and for securing both government and personal property.

6. Buildings. The Director of HECSA is responsible for all buildings on the HEC complex with the following exceptions:

a. Buildings 2592 and 2595, occupied by the Topographic Engineering Center (TEC) of the US Army Engineer Research and Development Center. The TEC Director is responsible for the security of these two buildings.

b. Building 2580, occupied by the US Army System Performance Office (USASPO). The USASPO Commander is responsible for the security of this building.

c. Building 2591, occupied by Central Intelligence Division (CID). The CID Director is responsible for the security of this building.

7. Security Force.

a. The security guard force consists of the following number and type of posts.

(1) Three 8-hour roving posts, 7 days a week.

(2) Six, 6-hour stationary posts in Building 2580, 7 days a week.

(3) Two, 12-hour stationary posts, one in Building 2593 and 1594, 5 days a week (Monday – Friday) excluding holidays.

(4) One, 8-hour stationary post in Building 2580, 5 days a week (Monday – Friday) excluding holidays.

b. The HECSA contract guard force is responsible for all buildings on the HEC complex except Building 2592 which is secured by the Defense Protective Service.

8. Entry Control.

a. Kingman Building (2593), Casey Building (2594).

(1) Normal Duty Hours. Access is authorized through doors that have controlled card access equipment. Access at specific doors and hallways are monitored and recorded with television cameras.

(2) Non-Duty Hours. Access is authorized through all doors that have controlled card access equipment. Cards are issued to personnel whose supervisor has approved them for access after duty hours.

b. Bunker (2591). This building has access control 24 hours a day, 7 days a week by a stand-alone alarm system maintained at the guards desk in the Kingman Building.

c. Supply (2582), Warehouse (2583), Motor Pool (2585) are open for business during normal duty hours. After normal duty hours, these buildings are secured with locks.

d. Fitness Center (2584). Building is unlocked and locked by the security guard force at specific hours that are subject to change and are convenient for employees. The center is not open on weekends and holidays.

9. General Area Security Requirements.

a. Lock all offices and storage rooms when no responsible member, permanently assigned to that office, is present.

b. Do not leave personal property such as wallets, purses, and radios unattended in unoccupied rooms.

c. Report all lost or stolen government or personal property immediately to the HECSA Security Office, 428-6479.

d. Account for government property in accordance with AR 710-2 and AR 735-5.

e. Report the following to the Guard Force, 428-6220, and the HECSA Security Manager's office 428-6479, immediately:

(1) Suspicious personnel, particularly those carrying suitcases or other containers, or those observing, photographing, or asking questions about the facilities or security measures.

(2) Unidentified vehicles parked or operated in a suspicious manner on or near the facilities.

(3) Abandoned parcels, boxes, or suitcases.

(4) Any other activity considered suspicious.

10. Threatcon Awareness Information.

a. NORMAL. Applies when the general threat of possible terrorist activity exists but warrants only a routine security posture.

b. ALPHA. Applies when there is a general threat of possible terrorist activity against personnel and installations, the nature and extent of which are unpredictable. Some measures are as follows:

- (1) Remind personnel to be inquisitive about strangers or unusual packages.
- (2) Watch for unidentified vehicles (ensure vehicles are registered).
- (3) Secure area not in regular use.
- (4) Increase spot checks of individuals entering the installation (foot roving patrol).

c. BRAVO. Applies when an increased or more predictable threat of terrorist activity exists. Some measures are as follows:

- (1) Move cars, trash container, etc., away from buildings.
- (2) Regularly inspect areas not in use.
- (3) Examine mail for letter or parcel bombs.
- (4) Remind drivers to lock and check vehicles.
- (5) Locking of all doors, except front. Control access with proper I.D. card and access card entry.
- (6) Security personnel manned.
- (7) Access card entry.

d. CHARLIE. Applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and installations is imminent. Some measures are as follows:

- (1) Strictly enforce control of entry. Randomly search vehicles.
- (2) Erect barriers and obstacles to control traffic flow.

e. 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 likely. Normally, THREATCON DELTA is declared as a localized warning. Some measures are as follows:

- (1) Identify all vehicles on the complex.
- (2) Search all vehicles entering the installation.
- (3) Search all suitcases, briefcases, and packages brought on the installation.
- (4) Minimize travel.

f. Local commanders retain the authority to implement terrorist threat measures (THREATCON Measures) to defend against a greater than expected terrorist threat; local commanders should not implement measures less rigorous than those appropriate for the declared THREATCON level for their particular facility. IF LOCAL CONDITIONS WARRANT GREATER PROTECTION, LOCAL COMMANDERS MAY ADOPT HIGHER THREATCON MEASURES THAN ORDERED BY THE CHAIN OF COMMAND.

11. Close of Business Office Check. Each Commander or Director of each activity on the HEC complex will ensure that each staff office and/or separate office will conduct a close of business office check.

a. Classified Material and Containers.

(1) Lock all classified containers and display the "CLOSED" or "LOCKED" reversible sign. Complete SF 702, Security Container Check Sheet, for each classified container.

(2) Ensure the tops of all of classified containers are free of extraneous materials.

(3) Check the area around desks, file cabinets, and security containers to determine that no classified material has fallen on the floor or between items of equipment.

b. Non-Classified Items.

(1) Turn off all electrical appliances, (coffee pots, hot plates, and microwaves) radios, televisions, computers and room lighting.

(2) Secure all highly pilferable items (laptop computers, calculators, cameras, coffee funds, and personal items). These items should be placed in lockable desk drawers or cabinets.

(3) Check and lock supply cabinets and storage areas.

12. Key and Lock Control.

a. The HECSA Maintenance and Transportation Branch must provide keys and locks for all organizations on the HEC complex. Keys will be issued only to designated key control custodians for each organization, staff office, or separate offices. Adequate control of keys will be maintained at all times.

b. Each organization, staff office, or separate office must appoint in writing, a primary and alternate key control custodian. A copy of the appointments will be provided to the CEHEC-LM Office. The key control custodians shall issue keys to their personnel. The issue of keys and locks will be kept to an absolute minimum needed to provide adequate security.

c. The CEHEC-LM Office must maintain a key control record of all keys issued. The log will reflect the number of keys issued, date of issue, the serial number of the keys, and name of the key control custodian to whom the keys were issued.

d. Each key control custodian must maintain a key control record of all keys issued. The log will reflect the number of keys issued, date issued, the serial number of the keys, and names of personnel permanently issued the keys.

e. All extra keys must be stored in an approved container when not issued. Keys signed out from the key box for emergency or temporary use must be returned immediately following use. The key to the key box should be in the possession of the key control custodian or alternatives as designated.

f. A written statement must be submitted immediately to the appropriate key control custodian stating the circumstances pertaining to the loss of any key. Requests for replacement keys, locks, or re-keying of locks must be supported by justification and forwarded to the CEHEC-LM Office.

g. Key control custodians must inventory all keys by serial number at least semiannually and will maintain a record on file for one year. A copy of the inventory must be provided to CEHEC-LM.

13. Information Systems Security.

a. Information Systems Security Manager (ISSM). An ISSM will be appointed by the Commander or Director to establish and implement the Information System Security (ISS) program in accordance with AR 380-19. The ISSM, for systems within their purview, will perform duties as follows:

(1) Oversee the execution of the ISS training and awareness program.

(2) Ensure that Automated Information Systems (AIS) are accredited to operate in accordance with AR 380-19.

(3) Ensure that each individual who possesses or has knowledge of information on the automated systems is responsible for protecting this information.

(4) Ensure that an Information Systems Security Officer (ISSO), Network Security Office(NSO), and Terminal Area Security Officer (TASO) are appointed as necessary, in accordance with AR 380-19.

(5) Maintain access control records and establish an access control policy in which only authorized personnel can gain access to the system.

(6) Establish a system for issuing, protecting, and changing system passwords.

b. All personnel will immediately report to the ISSM any attempt to gain unauthorized access to information, any system failure, or suspected defect which could lead to unauthorized disclosure.



CHARLES B. RAU
Director