



DEPARTMENT OF THE NAVY

NAVAL EDUCATION AND TRAINING CENTER

291 KOLLMEYER STREET

NEWPORT RHODE ISLAND 02841-1644

IN REPLY REFER TO:

NETCNPTINST 5530.5

Code 013

SEP 22 1999

NETCNPT INSTRUCTION 5530.5

Subj: PHYSICAL SECURITY AND LOSS PREVENTION PROGRAM

Ref: (a) OPNAVINST 5530.14C
(b) NAVSTANPT/Local Area Rhode Island Coordinator
Instruction 5530.3A
(c) CNETINST 5530.2G
(d) OPNAVINST 5510.36A
(e) OPNAVINST 5510.30A
(f) NETCNPTINST 7321.2E
(g) OPNAVINST 5239.1A

1. Purpose. To establish a physical security and loss prevention program for Naval Education and Training Center (NETC) pursuant to reference (a) and to support the Naval Station (NAVSTA) Newport/Local Area Rhode Island Coordinator for the subject program.

2. Discussion. Physical security is that part of security concerned with physical means and measures, both active and passive, designed to safeguard personnel and protect property by preventing, detecting and confronting acts of unauthorized access, espionage, sabotage, malicious damage and theft. Loss prevention is particularly concerned with preventing loss of supplies, tools, equipment or other materials in issue, use, storage and/or transit processes. Concern is not only focused on the threat of criminal activity and acts of wrong doing by forces external to the organizational unit, it is also specifically directed toward internal causes: theft and pilferage by those who have authorized access, lack of attention to physical security practices and procedures, and disregard for property controls and accountability.

3. Property. Property consists of all assets, including real property funds and arms, ammunition and explosives, tools and equipment, materials and supplies, computer hardware, software and related Automated Data Processing (ADP) equipment, and information in the form of documents and other media, whether categorized as routine or special, unclassified or classified, non-sensitive or sensitive, critical, valuable or precious.

4. Scope. Security orders and regulations issued by the Commanding Officer, NETC, pursuant to reference (a) and applicable laws of the United States will be effective throughout the physical premises of NETC. Every person entering into the area encompassed by NETC, as a visitor, for duty or employment, shall be subject to these regulations and shall, as appropriate, be familiar with all provisions thereof. The NETC Physical Security Review Council (PSRC) is responsible for developing the command's physical security and loss prevention program.

5. Jurisdiction. Pursuant to the applicable provisions of United States Code, whoever shall willfully violate any lawful regulation issued for the protection or security of facilities of the Department of Defense may be found guilty of a misdemeanor and, upon conviction thereof, shall be liable for a fine not to exceed \$10,000 or imprisonment for not more than one year or both. Military personnel are subject to prosecution under the provisions of the Uniform Code of Military Justice.

6. Security Responsibilities. Security is the direct, immediate, legal and moral responsibility of all persons in, and employed by the command. Specific responsibilities are set forth in the following articles:

a. Commanding Officer. The Commanding Officer is overall responsible for physical security. He or she is responsible for appointing a Physical Security Officer and for establishing and maintaining a Physical Security and Loss Prevention Program to include an Anti-Terrorist and Physical Security Training Program, Key Control and Plant/Minor Property Control Programs. The Commanding Officer will provide sufficient resources, staff assistance and authority to the Physical Security Officer to implement, manage and execute an effective Physical Security and Loss Prevention Program.

b. Executive Officer. The Executive Officer assists the Commanding Officer as directed. In addition, the Executive Officer directs the command Loss Prevention Program by appointing members of the Physical Security Review Committee to the Loss Prevention Sub-committee as appropriate.

c. Physical Security Officer. Assists the Commanding Officer in determining the adequacy of the Command Physical Security and Loss Prevention Programs by identifying those areas in which improved physical security and loss prevention measures are required and by managing the program. The Physical Security Officer will be:

(1) An officer, senior enlisted (E7/8/9), or civil Service employee GS-9 or higher.

(2) Designated in writing by the Commanding Officer, with the billet identified as a principal or sole collateral duty.

(3) Familiar with the provisions of this instruction, as well as with references (a) through (c).

(4) Provided sufficient resources, staff assistance and authority to manage and carry out an effective Physical Security and Loss Prevention Program.

(5) Assigned concurrently as the Security Manager if required. The Physical Security Officer will (not all-inclusive):

(a) Manage, implement and direct the command's Physical Security and Loss Prevention Programs.

(b) Determine the adequacy of the command's Physical Security and Loss Prevention Programs and identify those areas in which improved physical security and loss prevention is required.

(c) Implement and maintain the current command physical security plan.

(d) Implement and maintain the command's physical security instruction which addresses required physical security procedures.

(e) Establish a personnel identification and access control system where required.

(f) Conduct an annual physical security survey.

(g) Attend all NAVSTA physical security briefings.

(h) Coordinate physical security requirements with NAVSTA or other tenant activities and ensure such requirements are set forth in appropriate host tenant, interservice support and licensing agreements.

(i) Participate in planning, direction, coordination and implementation of procedures for crisis management of situations (including hostage situations) which pose a threat to the physical security of the command, and provide advice to the Commanding Officer during crisis which apply to physical security.

(j) Serve as command liaison officer with the Naval Criminal Investigation Service (NCIS) and other federal, state and local authorities in matters pertaining to physical security.

(k) Maintain contact with and solicit advice from the cognizant staff judge advocate concerning legal aspects of physical security.

(l) Maintain regular contact and collaborate with managers of specialized security programs within the command concerning physical security threats and requirements.

(m) Act as chairperson of the Physical Security Review Committee, schedule meetings, notify appropriate personnel, and be responsible for minutes and records of the command Physical Security Review Committee.

(n) Establish and provide for the maintenance of records relating to losses of government and personal property and violations and breaches of physical security measures and procedures.

(o) Conduct other appropriate physical security duties and training as may be required.

d. Security Manager. The Security Manager is the Commanding Officer's advisor and direct representative in matters pertaining to the security of classified material as per references (d) and (e). In so doing, the Physical Security Officer operates in support of the Security Manager in protecting classified material.

e. Senior Watch Officer. The Senior Watch Officer (SWO) will carry out general military training for all watchstanders as determined by the commanding officer. The SWO will coordinate with the Physical Security Officer in the conduct of physical security training and with the Security Manager concerning the handling and safeguarding of classified material.

f. Command Duty Officer. The Command Duty Officer (CDO) will be familiar with provisions of this instruction and references (a) through (c). The CDO will support, coordinate and act as liaison with the Naval Station appointed representatives in all matters pertaining to physical security. The CDO will report and document all violations of the command's physical security program as appropriate.

g. Command Facility Manager. Makes recommendations and coordinates with Public Works and civilian contractors any required changes in command facilities needed to support the Physical Security Program.

h. Plant and Minor Property Custodian. The Plant and Minor Property Custodian will conduct an annual inventory of all command-controlled materials as per reference (f) and present findings to the Physical Security Officer.

7. Physical Security Review and Assessment.

a. Since Physical Security Review and Assessment is an ongoing process that all NETC personnel share, it is the responsibility of ALL HANDS to immediately report to the Physical Security Officer, any material discrepancies or security deficiencies noted in a NETC occupied facility which could impact command security. The Physical Security Officer will take prompt action to correct any material discrepancy or

security deficiency reported. If the material discrepancy or security deficiency cannot be corrected immediately, adequate controls will be effected until repairs are completed or a thorough assessment and permanent policy adopted.

b. The Physical Security Officer will conduct an annual Physical Security Survey of all NETC facilities using reference (a) to include material condition of security measures in place (cipher locks, door locks, windows, etc.) effectiveness of Key Control Program and Badge and Access Control System. Additionally, access lists must be verified for currency and accuracy, and restricted areas must be properly posted as such. The Physical Security Officer and the Facility Manager will work closely together to correct any noted material discrepancies. A copy of the completed survey will be forwarded to NAVSTA Security Office.

c. The Security Manager, Automated Information Systems Security Officer and all other special security officers assigned will assist and support the Physical Security Officer in conducting the annual Physical Security Survey.

d. The Physical Security Officer will review all Missing, Lost, Stolen, and Recovered (MSLR) Government Property Reports of significant losses and breaches of security, and, based on the analysis of such instances, recommend improvements to the Physical Security and Loss Prevention Programs. The Physical Security Officer will ensure copies of the MSLR's are forwarded to the NAVSTA Security Officer.

e. All administrative changes to the Physical Security Program which result from a Security Survey, such as designating a new restricted area or changing the level designation of an existing area will be submitted to the Commanding Officer for final approval. The Physical Security Officer and Facility Manager will ensure any changes made are in accordance with reference (a) and subsequently incorporated into the NAVSTA instruction.

f. The Security Officer maintains all records until the completion of the cognizant Inspector General command inspection cycle.

8. Force Protection and Threat Assessment.

a. NAVSTA, as per the inter-service agreement, will conduct Threat Assessments and determine the security posture of the Base. They will deploy security assets to best protect designated areas and provide overall perimeter and area security for NETC.

b. NETC will immediately notify designated NAVSTA personnel of any situation or information that could impact the security posture of the Base.

c. NETC will comply with all reasonable requests and comply with NAVSTA Physical Security and Force Protection Programs.

d. NETC will provide a fair share of qualified personnel to support the NAVSTA Auxiliary Security Force (ASF). NAVSTA is responsible to train, equip, and deploy the ASF as required.

e. NAVSTA will exercise all tactical control over emergency services and any security assets that may be required. Appointed NETC representatives (i.e. Command Duty Officer, Staff Duty Officers, Physical Security Officer, Security Manager, etc.) will work closely with NAVSTA personnel and provide support as required.

9. Security and Anti-terrorist Training Program.

a. The Physical Security Officer is responsible for ensuring that all NETC personnel receive annual training on the Physical Security and Loss Prevention Program and Anti-terrorist Training. The Security Officer will work closely with the Command Training Officer to ensure all personnel receive the required training and that it is adequately documented.

b. All NETC Staff and students on station for greater than 30 days, will receive an initial security brief as part of the check-in process.

c. The requirement for annual security and anti-terrorist training for NETC Staff and Student personnel will be integrated into the existing General Military Training (GMT) Program.

d. A qualified instructor will conduct required anti-terrorist training for overseas screening. School Directors/Department Heads will ensure a sufficient number of qualified instructors are available to meet their requirements. Students will receive the training as either part of the formal curriculum or as adjunct training. All training will be properly documented as required.

e. Staff personnel requiring the Anti-terrorist Brief as part of the overseas screening process will contact the Physical Security Officer who will maintain a current list of qualified instructors and will ensure arrangements are made for required training.

10. Key and Lock Control Program.

a. The key and lock control program for NETC as required by references (a) through (c) includes all keys, combination push-button locks, and locking devices used to protect or secure classified material, sensitive material, controlled items and supplies. This plan does not include keys, locks and padlocks for convenience, privacy, administrative or personal use.

b. Procedures.

(1) Accountability. All school directors/department heads will appoint a Key Control Officer for spaces and buildings under their cognizance as follows:

| <u>Building</u> | <u>School/Department</u> |
|--|--|
| Perry Hall Bldg. 440 (except Command Leadership School) | Command Facility Manager |
| King Hall Bldg. 291 (Command Area) | Command Facility Manager |
| King Hall Bldg. 291 (except Command Area) | OIS |
| Nimitz Hall Bldg. 197 Bldg 1112 | BOOST BOOST |
| Kay Hall Bldg. 1801 Bldg. 85 | Command Facility Manager Communication School |

| | |
|-------------------------|----------------------|
| Bldg. 114 | Chaplain School |
| Training Pool Bldg. 307 | Damage Control Dept. |
| Buttercup Bldg. 403 | Damage Control Dept. |
| Bldg. 1275, 1276, 1277 | Damage Control Dept. |

(2) Key Control. The Key Control Officer will institute a program that lists: all keys on hand; key issuance sign-out, date and time issued and returned; and signatures of persons drawing or returning keys. Access to the Key Control Area must be controlled and the space must be secured when not in use. When not attended or used, keys shall be secured in containers with working locks. Continuous accountability of keys is required at all times.

(3) Issue of Master Keys. Master keys will only be issued at the discretion and approval of the school director or department head. A duty master key may be provided for the SDO/CDO.

(4) Criteria for Issuing Keys. Keys issued for reasons of physical security may be issued to staff members with a legitimate requirement for access upon reporting on board NETC. The Key Control Officer will issue and the member will sign for the receipt of each key(s). Students should not be issued keys.

(5) Key Turn-In. Prior to transfer from NETC, all staff members will return issued keys to the Key Control Officer and sign a custody document to indicate key was returned. The Key Control Officer will then sign for the receipt of the key.

(6) Lost, Misplaced or Stolen Keys. In the event of a lost, misplaced, or stolen key(s), the Key Control Officer will be notified as soon as possible and re-keying of the applicable door will be initiated. If the missing key is a master, the school director/department head will also be notified.

(7) Inventories. The Key Control Officer will conduct an annual inventory of all keys issued. All keys will also be inventoried upon change or transfer of the Key Control Officer.

(8) Duplicates. The unauthorized duplication of controlled keys is strictly prohibited. Only the Key Control

Officer may make additional copies of keys if required and only school directors/department heads may authorize duplication of master keys.

(9) Cipher Locks. Command personnel who have in their spaces doors that contain or are equipped with cipher locks will have on file a documented list of all users who possess the combination. The cipher lock combination shall be changed at least annually or whenever a person authorized access transfers.

11. Area Security. Areas, building(s) and other structures on NETC which are designated as restricted are listed below:

a. Level One Areas. A Level One restricted area is the least secure and serves as a buffer zone for Level Two and Level Three areas. This area contains:

(1) A personnel identification and control system.

(2) Ingress and egress controlled by guards or other appropriately trained personnel.

(3) Procedures to control entry into the area by individuals (military, civil service, contractors, official visitors) who require access for reasons of employment/official business; individuals who render service (vendors, delivery people); dependents; retired military; and unofficial visitors.

(4) The only NETC asset designated as a Level One restricted area is Communication School, Bldg. 85 with Level Two restricted areas within.

b. Level Two Areas. A Level Two restricted area is the second most secure area. It may be inside a Level One area, but is never inside a Level Three area. It contains a security interest which, if lost, stolen, compromised, or sabotaged would cause serious damage to command mission or national security. Uncontrolled or unescorted movement could permit access to classified interests. The following minimum security measures are required for all Level Two restricted areas:

(1) A clearly defined and protected perimeter, as outlined in reference (a).

(2) A personnel identification and control system. An activity area pass/I.D. or military/civilian government identification card must be displayed at all times on the outer garment or inside the clothing when the I.D. may present a safety hazard. In those cases, the identification must be available on the person; e.g., in a pocket, under an outer garment, etc. During normal working hours, use of an access list and entry/departure log is suggested. Access to the area must be logged in/out for those personnel who are not on the access list.

(3) Admittance of only those who have duties requiring access and are granted appropriate security authorization. Persons who have not been cleared for access may, with appropriate approval, be admitted to such area, but they must be controlled by escort and the security interest protected from compromise or other degradation.

(4) When secure, a Level Two area with an Intrusion Detection System (IDS), such as Communication School, requires a check at least once every eight hours for signs of unauthorized entry or other activity which threatens to degrade Level Two Area security. For purposes of this instruction, the nightly security checks conducted by the NAVSTA Security Personnel may fulfill this requirement.

(5) The following facilities at NETC are designated Level Two areas in Communication School, Bldg. 85:

- | | |
|---------------|-----------------------------------|
| - Rm. 111 | CMS Vault |
| - Rm. 206 | Naval Warfare Publication Library |
| - Rm. 209/210 | EKMS Classroom |

c. Level Three Areas. A Level Three restricted area is the most secure type of restricted area. Uncontrolled or unescorted movement constitutes access to security interest. NETC has no Level Three areas.

12. Badge and Access Control System.

a. Issue guidance for the implementation of security badge systems for those buildings and spaces designated as Level One and Two restricted areas.

b. The following guidance has been established to prevent unauthorized access to NETC restricted areas.

(1) All staff, students, civilian employees, and visitors entering NETC restricted areas are required to display appropriate badges as necessary.

(2) Designated administrative and duty personnel (when posted) are responsible for issue and control of security badges. Authorized NETC staff personnel will be issued security badges by the Security Manager.

(3) Access to NETC restricted areas is limited to individuals with either a designated NETC security badge, or with prior arrangement and badge clearance codes verified, a Surface Warfare Officer School Command or a Naval War College security badge. Any student or visitor entering or departing an NETC designated restricted area must sign in/out at the designated control point. After hours is defined as between 1800 and 0600 on weekdays and on all day on Saturday, Sunday and holidays.

(4) NETC serialized staff security badges will have a current photograph and an expiration date corresponding to the individual's projected rotation date.

(5) Students and visitors will wear security badges on the upper body while in NETC restricted areas in such a manner as to be clearly visible. All properly cleared NETC staff members whose name appears on the approved access list for the specific designated Level One areas may be granted access to the restricted area based on personal recognition. Staff members are required to wear their security badges whenever entering, working in or visiting designated Level Two restricted areas.

c. Applicability.

(1) NETC staff members who require access and have been granted the necessary interim or final security clearance will be issued the appropriate NETC staff security badge.

(2) Students will be issued a Student Badge once authorizing clearance information has been received from their parent command or Department of the Navy Central Adjudication Facility (DONCAF). Student badges will be issued by the school director (or designated representative) providing the training.

(3) Visitors will be issued either the "Escort required" or "No Escort required" visitor badges.

(a) Visitors will be issued a "No Escort Required" Visitor Badge after clearance information has been received from their parent command or DONCAF. Personnel must be cleared to at least Interim Secret. Personnel issued a "No Escort Required" Visitor Badge will still require an escort if their duties require access to a Level Two restricted area.

(b) Visitors will be issued an "Escort Required" Visitor Badge when no clearance information exists. Personnel issued this type badge require escort at all times.

(4) Designated administrative and duty personnel (when posted) will log all visitors into a logbook, issue a badge and arrange for an escort (if necessary). Upon completion of the visit, the badge will be recovered, returned to the badge box, and logged out.

(5) Positive control of all un-issued security badges will be maintained at all times. All visitor badges will be inventoried and accounted for at the end of the normal workday or prior to securing a restricted area or facility. The Security Manager will be notified if any security badge is discovered missing and take appropriate action.

13. Intrusion Detection System (IDS).

a. Purpose.

(1) Permit more economical and efficient use of security personnel through the employment of mobile responding security forces instead of fixed guard posts and/or patrols.

(2) Provide additional controls at critical areas or points.

(3) Enhance the security capability to detect and defeat intruders.

(4) Provide the earliest practical warning to security forces of any attempted protected area penetration.

b. Background. The following established guidance stipulates the responsibilities for maintenance, operation and monitoring of an IDS system.

c. Policy.

(1) All restricted areas, which meet the criteria for the installation of an Intrusion Detection System, will have a system installed that complies with reference (a).

(2) As per existing agreement, NAVSTA will be responsible for monitoring (24 hours a day) and responding to all IDS alarms, which terminate at police headquarters.

d. Action.

(1) NETC will notify NAVSTA of any additional security requirements not already installed or in place, which may be required to secure restricted areas and materials.

(2) NAVSTA is responsible to provide an IDS system that conforms to specifications outlined in reference (a). They will provide automatic/back-up emergency power, electronic line supervision for transmission lines, audible/visual alarm indications, routine/emergency maintenance, and a record of maintenance, testing, malfunctions and false alarms.

(3) NETC personnel are required to immediately notify NAVSTANPT of any discrepancies discovered which degrade the effectiveness of an installed IDS system.

(4) NAVSTA will provide routine building security checks of all designated buildings after working hours at random times, not to exceed an eight-hour interval.

(5) NAVSTA will respond to all IDS alarms with sufficient assets to protect restricted areas and materials from compromise.

(6) Communication School, as the only NETC school requiring an IDS system, will adopt a local policy for the day to day operation of IDS systems installed to protect access to designated restricted areas. The procedure should designate authorized IDS operators, provide training for IDS system(s), and procedures in the event of IDS system failure.

(7) Designated Communication School personnel will ensure all restricted areas are secure and installed IDS alarms set when the building is secured after working hours.

(8) Any malfunctions, failures, or deficiencies with the IDS system will be reported promptly to the Security Manager for appropriate action.

14. General Physical Security Policies.

a. All buildings will be secured after normal working hours to prevent unauthorized access. School Directors/Department Heads are responsible to establish normal procedures for day to day operations sufficient to protect facilities and command assets under their cognizance.

b. All offices, classrooms, storage spaces or any other spaces which contain minor and plant property as defined by reference (f), particularly ADP equipment and spaces, will be secured when not occupied by authorized personnel.

c. When securing spaces which contain ADP equipment, before physically securing the area, computer users will follow defined "log-off" procedures to maintain information integrity per reference (g).

d. Plant and Minor Property Custodians and Information System Security Officers (ISSO's) will maintain current, accurate inventories of all equipment per reference (f). These inventories will assist in quickly identifying missing or damaged equipment.

e. All areas identified as gender-specific are off limits to the opposite sex. Procedures that conform to DOD and Navy policy will be in place to admit authorized personnel to conduct official business.

f. The BOOST SDO will ensure that Perry Hall (Bldg. 440), Kay Hall (Bldg. 1801) and Bldg. 1112 are secured prior to 2200 each workday and when not in use on weekends and holidays.

g. The NETC CDO will be notified of any NETC assets that are discovered to be unsecured after normal working hours. An appropriate investigation and a CDO Log entry will be made.

h. Any building security devices, such as door locks, padlocks, electronic door keypads etc. which are discovered to be faulty or unserviceable, will be reported to the Command Facility Manager and an emergency service call made to NAVSTA Public Works Department. If the device cannot be repaired during normal working hours, the NETC CDO will be notified and appropriate action taken.


P. A. DRISLANE

Distribution:
Lists I & II