UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION
POSTAL SERVICE CENTER BOX 8003
CHERRY POINT, NORTH CAROLINA 28533-0003

IN REPLY REFER TO:
ASO 1610.6C
SES
14 JUN 201

AIR STATION ORDER 1610.6C

From: Commanding Officer
To: Distribution List

Subj: PHYSICAL SECURITY AND CRIME PREVENTION PROGRAM

Ref: (a) MCO 5530.14A, Physical Security Program
(b) UFC 4-022-01 Entry Control Facility
(c) UFC 4-021-02 Electronic Security Systems
(d) ASO 5530.2D Flight Line Security Program
(e) UFC 4-025-01 Waterfront Security Engineering
(f) ASO 5530.4, Emergency Mass Notification System
(g) ASO 5560.6A, Installation Access
(h) ASO 3058.1, Mission Assurance Program

Encl: (1) Station Perimeter Security Supplement
(2) Electronic Security Systems Supplement
(3) Asset Protection Supplement
(4) Crime Prevention Programs Supplement
(5) Physical Security Working Group Supplement
(6) Request for Marine Corps Electronic Security System
(7) Request for Personal Identification Number (PIN) Issuance for (Building/Area)

1. Situation. An active installation physical security program is the bedrock on which many other security programs are anchored. The physical security/crime prevention program is designed to prevent or mitigate the potentially deleterious effects of criminal and/or terrorist activity. This Order establishes physical security and crime prevention guidance and procedures for the Crime Prevention Program and establishes physical security standards for safeguarding unclassified and non-sensitive government supplies, equipment, and personnel.

2. Cancellation. ASO 1610.6B.

3. Mission. On a continuing basis, MCAS Cherry Point implements active and passive physical security measures presenting an installation security profile commensurate with the threat, in

order to achieve antiterrorism (AT) readiness, safeguard personnel and property against unauthorized access, espionage, sabotage, wrongful destruction, malicious damage, theft, pilferage, and other acts which degrade mission readiness.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. To implement aggressive active and passive security measures that elevate our security posture commensurate with the threat. The installation will establish defense in depth measures with priority of effort at the entry gates and the perimeter of the installation. End state: Passive and active physical security measures are in place which deter or mitigate the potentially harmful effects of criminal/terrorism activity.

(2) Concept of Operations

(a) Pre-Incident. References (a) and (b) establish security guidelines for the protection of personnel and assets forming the crux of day-to-day physical security. These physical security measures are designed to establish a baseline physical security posture and include physical security surveys, elevating individual awareness, developing and practicing good security procedures, considering AT concerns into new building design, training security forces, implementing random increased security measures, and varying security routines. This phase is complete when a criminal/terrorist activity has occurred.

(b) Incident. This phase involves immediate correction of the security deficiency or implementing mitigating security measures, commensurate with the threat, which reduces the likelihood of further criminal/terrorist activity. This phase is complete when the immediate threat or security concern has been abated.

(c) Post-Incident. This involves examining the events that allowed the incident to occur and developing security measures to lessen the likelihood it will happen again. This phase is complete when lessons learned have been applied to correct the deficiency.

b. Subordinate Element Missions

(1) Tasks

(a) Operations Directorate

1. Take the lead in coordinating/integrating the physical security program requirements with the AT program.

2. Per reference (h), establish and coordinate a Mission Assurance working group structure that facilitates the discussion and mitigation of physical security issues.

3. Work with PMO to incorporate Physical Security items into MA working groups and executive forums in order to meet the requirements of the Physical Security Council and Physical Security Working Group.

4. Ensure all AT deficiencies are entered/ forwarded to the proper avenue for corrective action.

~~(b) Mission Assurance Program Executive Committee (MAPEC)~~

~~1. Establish Mission Assurance Working Group (MAWG) to address physical security, crime prevention, and anti-terrorism actions.~~

~~2. Review and prioritize installation physical security and AT corrective actions.~~

~~3. Using the current installation threat assessment and lessons learned to evaluate the effectiveness of current security programs and make recommendations to the CO or XO, MCAS Cherry Point concerning priorities for the commitment and allocation of resources and funds.~~

~~d. Evaluate any reports of large losses or thefts of government property of more than $1,000 in value and take corrective action.~~

~~e. Review existing regulations, directives, and plans to ensure the installation can support the Mission Assurance plan.~~

(b) Security and Emergency Services

1. Ensure that all commands/units/organizations are complying with all physical security requirements and regulations.

2. Establish and maintain the command's physical security program per reference (a).

3. Ensure physical security construction requirements are met in accordance with reference (a).

4. Conduct Physical Security and Crime Prevention surveys in accordance with reference (a).

5. Control access into the Air Station in accordance with reference (g).

6. Provide the reactionary force for Marine Corps Electronic Security System (MCESS) alarm activations.

7. Provide operational security and ensure maintenance tasks are completed for MCESS in accordance with reference (a).

8. Publish and staff a list of units/commands/ organizations with identified physical security deficiencies and status of corrective action reports. The list will be submitted annually by 30 April.

9. Review all plans for new construction or major building modifications to ensure all security requirements are being met.

10. Evaluate the results of Physical Security related inspections, surveys, and exercises and recommend corrective action.

11. Review installation entry and visitor control procedures.

12. Develop security education requirements.

13. Provide a representative to the MAWG and MAEC to serve as a coordinator for all Physical Security issues in order to meet PSCB and PSWG requirements.

14. Maintain a Station Operation ID program.

15. Ensure that all Physical Security Specialists are trained and certified in accordance with reference (a).

16. Provide units/commands assistance in setting up unit level crime prevention programs.

17. Provide unit level crime prevention briefs as requested.

18. Take the lead in developing and implementing a waterborne security plan.

(c) Subordinate and Tenant Commands

1. Assign, in writing, a unit Access Control Officer. All unit level Access Control Officers will submit monthly by name flight line access rosters to the Provost Marshal, Attn: Badging Office, Pass & ID. Unit Access Control Officers will designate, in writing, all personnel who require access to unit restricted areas and issuance of PIN Codes for MCESS IDS.

2. Assign, in writing, a Command Security Officer who will have the authority to implement, manage, and execute a unit level physical security program.

3. Maintain security of assigned spaces, supplies, and equipment following the guidelines set forth in enclosure (4).

4. Maintain security of arms, ammunition, and explosives in accordance with reference (a).

5. Include the Provost Marshal's Office in the distribution for all Missing, Lost, Stolen, Recovered (MLSR) reports.

6. Review all crime prevention and physical security surveys for your respective unit and ensure corrective action is taken on all noted deficiencies. Results will be forwarded in the form of a Corrective Action Report to Physical Security, via the Provost Marshal, within 90 days of conducting the annual physical security survey.

7. Identify all Critical Infrastructure and Restricted Areas, in writing, and submit unit level annual Restricted Area Letter to Station Commanding Officer, via the Provost Marshal, to ensure proper security measures are coordinated and being met. Restricted Areas letters are due to the Provost Marshal annually by 30 November.

8. Per reference (h), provide membership to the Air Station MAWG to coordinate physical security requirements and corrective actions of physical security deficiencies.

9. Develop and submit to Physical Security, via the Provost Marshal, tenant organization Physical Security Plans.

10. Develop written perimeter security procedures and access control procedures for buildings and areas under their control.

11. Per reference (h), participate in the MAWG and take the lead in integrating the physical security and AT program requirements for their command/unit/organization.

(d) Facilities Directorate

1. Per reference (h), participate in the MAWG and MAEC and take the lead in integrating the physical security and AT program requirements in with the facility and building construction code requirements.

2. Integrate physical security and AT construction requirements into the Facilities Sustainment Model for program planning and budgeting.

(e) Logistics Services Directorate

1. Locate and move any/all barriers as required to meet station barrier plan.

(f) Marine Corps Community Services (MCCS)

1. Per reference (h), participate in the MAWG and take the lead in integrating the physical security and AT program requirements for MCCS facilities.

2. Integrate AT plans and programs with the MAWG and MAEC.

5. Administration and Logistics. This Order can be accessed via the Station Adjutant's website.

6. Command and Signal

a. This Order is applicable to subordinate and tenant commands aboard MCAS Cherry Point.

b. This Order is effective the date signed.

T. W. FERRY

Station Perimeter Security Supplement

PERIMETER SECURITY REQUIREMENTS: This section contains information and guidelines specific to the perimeter security of MCAS Cherry Point and the outlying areas assigned to this command. All requirements in this section will be applied to the following areas: MCAS Cherry Point, MCALF Bogue Field, MCOLF Atlantic Field and Piney Island, and MCOLF Oak Grove.

1. Perimeter Security Controls

a. Fencing. Ensure that all station property boundaries meet the minimum security requirements and construction standards as set forth in reference (a).

(1) All station perimeter fencing that can reasonably be threatened by high speed vehicular approach will be reinforced with ¾" steel cable per reference (a).

(2) All clear zones will be maintained in accordance with reference (a). Any discrepancies will be reported to Facilities Maintenance for corrective action via work request or R-1 submission.

b. Entry Control Points (ECP). When open, all ECP's will be manned by trained armed guard personnel in accordance with reference (a). Reference (b) provides construction requirements and anti-terrorism standards for perimeter ECP's. All ECP's will be reinforced by ¾" steel cable per reference (a). Identified deficiencies will be submitted to the MAWG for addressing and submission to the MAPEC for review. The primary ECP's are as follows:

(1) Gate 1 Main ECP. Primary entry control point for the station and is open 24 hours.

(2) Gate 2 Cunningham ECP. Located on Cunningham Boulevard, this gate is open during morning and afternoon rush hours, special events, or when an alternate entry point is required for Gate 1.

(3) Gate 27 Slocum ECP. Located on Slocum Road, this gate is closed Monday through Thursday from 2200-0600 and 0100-0600 Friday through Sunday.

(4) Gate 29 Catawba ECP. Located within Nugent Cove Housing, this gate remains secured except for periods in the

morning and afternoon and is restricted to school bus traffic or exiting POV's. No POV entry is permitted.

(5) Gate 809 (6th Ave. & "A" Street). Primary gate for the Flight Line Restricted Area and the only manned gate to access the Flight Line. This gate is open 24 hours.

(6) Bogue Field Gate. Open in support of operations, manned 24 hours.

(7) Atlantic Field Gate. Opened as needed in support of operation. Security requirements at this location are subject to change per the Commanding Officer or threat level.

(8) Oak Grove Gate. Opened as needed in support of operations. Security requirements at this location are subject to change per the Commanding Officer or threat level.

2. Waterborne Security Patrols

a. A large amount of the MCAS Cherry Point perimeter borders waterways and presents a unique security challenge that requires coordination with outside agencies.

b. See reference (h) for MCAS Cherry Point waterway security procedures.

c. All waterway security patrols of the waterways will be conducted by Security and Emergency Services (SES) by trained and equipped security personnel.

(1) Develop and publish waterborne security patrol zones.

(2) Develop a waterborne security communications plan.

(3) All waterway security patrols will be conducted utilizing government owned water craft.

(4) Maintain an appropriate number of qualified boat personnel to conduct waterborne security operations.

(5) When conducting waterway security patrols, Cherry Point Police will be armed and maintain security communications with SES Dispatch.

(6) Any deficiencies in signage or waterway barriers will be reported to Physical Security, who will initiate corrective action via work order or R-1 submission.

(7) Waterway patrol normal operations will be supplemented with additional patrols per the monthly Random Antiterrorism Measure schedule.

d. All waterway boundaries will be marked with appropriate "Warning Government Property" signs every 200 feet. All signs will be posted as to be readable from off station.

e. PMO will be prepared to conduct all waterborne security action sets identified in the Waterside Security FPCON Action Sets per reference (h).

f. The waterway Intrusion Detection System consists of the JIGSAW system, which consists of 5 radar based units with integrated motion activated closed circuit television (CCTV) designed to detect movement within the outlined waterway zones. The TASS annunciates at the PMO ACC and provides CCTV for assessment of alarms. This system is maintained by the Physical Security Section of the Provost Marshal's Office. The JIGSAW radar units are located at the following five locations:

(1) Ordnance Point

(2) Pelican Point

(3) Golf Course

(4) Navy Boat Docks

(5) Food Plot Trail

Electronic Security Systems Supplement

Marine Corps Electronic Security System (MCESS): The MCESS is a comprehensive system that includes automated access control (AACS), intrusion detection, closed circuit television (CCTV), and Mass Notification Systems (MNS) designed to enhance the capabilities of security forces. Operation, management, and maintenance of the station MNS is covered in reference (f). The MCESS is located within the Provost Marshal's Office Alarm Control Center (ACC), which is continuously manned and monitored.

1. Automated Access Control System (AACS)

a. The only authorized credentials that can be utilized in the MCESS AACS are a Common Access Card (CAC), locally produced MCESS credential, or Personal Identity Verification (PIV) credential.

b. All personnel who require automated access will report to the Badging Office, Pass & ID, to have their credentials read into the MCESS.

c. It is the unit/command/company's responsibility to appoint, in writing, a unit Access Control Officer (ACO). The ACO will be responsible to ensure that all personnel who require automated access entry to an area have been assigned in writing. Properly signed access letters are then forwarded to the Badging Office, Pass & ID.

d. Personnel without properly signed written authorization by a designated ACO will not be granted automated access entry into a designated Restricted Area.

e. The AACS is maintained by the Provost Marshal's Office Physical Security section. In the event of a vehicle gate/turnstile malfunction, the adjacent squadron may opt to either post a trained and equipped guard or direct their personnel to another gate for entry.

2. Intrusion Detection System (IDS)

a. The MCESS will be the only IDS used aboard the installation. No non-MCESS IDS will be monitored by PMO. Physical Security will not approve any requests for installation of non-MCESS IDS.

b. Employing the MCESS does not eliminate the requirement for the unit to develop, publish, and maintain a robust unit physical security program that includes access control, security checks, and contingency plans for when MCESS fails or is down for routine maintenance.

c. The MCESS will be monitored by PMO at the Alarm Control Center (ACC), which will be designated as a Restricted Area in writing. The ACC will have access control on all entry doors, either by cypher locks, CAC reader, or emergency exit only hardware.

d. All requests for MCESS installation will be submitted to physical security, in writing, for review. The written request will include, at a minimum, regulatory requirement for system and unit funding availability. Requests that do not include a regulatory requirement will not be considered. The request letter will be signed by the unit Commanding Officer or personnel with by direction authority.

e. All MCESS testing and maintenance will be performed in accordance with reference (a). All IDS drills will be coordinated with Physical Security prior to conducting the drill.

f. The acceptable nuisance rate for MCESS aboard the Air Station is zero. All system malfunctions will be recorded and reported to SPAWAR for corrective action.

3. Closed Circuit Television (CCTV)

a. CCTV will only be used to assist or enhance the abilities of security forces. The employment of motion activated CCTV as a tool to assess alarm activations is encouraged, but not required.

b. All CCTV that will be monitored by PMO at the ACC will be part of the MCESS.

c. All requests for CCTV to be monitored by PMO will be forwarded, in writing, to Physical Security for vetting and submission to MCICOM for consideration. The written request will include, at a minimum, regulatory requirement for system and unit funding availability. Requests that include no regulatory requirement will not be considered. The request letter will be signed by the unit Commanding Officer or personnel with by direction authority.

Asset Protection Supplement

ASSET PROTECTION: This section provides basic crime prevention steps that individuals and units can take and minimum security requirements based on the type of asset being protected and the location it is being stored at. The purpose of this supplement is to assist in the reduction of crime.

1. Barracks Crime Prevention

a. Register high value property owned by personnel residing in the barracks by utilizing "Operation I.D." or similar programs. A record of model and serial numbers will enhance the potential for recovery of property and conviction of the thief. Inexpensive electric engravers are available through normal supply channels or may be checked out at PMO. The forms for Operation I.D. can be obtained at PMO and after being completed are retained in the individual's Service Record Book or another location designated by the unit.

b. Initiate procedures for securing the property of personnel on leave, TAD, or field duty.

c. Require all valuables to be secured in a wall locker when the occupant is not in his/her room. Seventy five percent of all larcenies involve property left unsecured and unattended.

d. Require duty NCOs to make frequent security checks of their assigned areas. Such duty personnel should be held strictly accountable for their assigned areas and for failing to take action to correct security violations, such as unsecured lockers or valuables left unsecured or unattended. Duty personnel should be provided with extra locks for use in securing unattended lockers. Requiring each watch stander to make hourly log book entries concerning the security of their assigned area is a must and will help to ensure the integrity of each watch stander.

e. Establish a system of visitor control where all visitors are logged in and out by the Duty Non-Commissioned Officer (DNCO) and escorted by the resident they are visiting.

f. Ensure that adequate serviceable wall lockers are provided for barracks residents.

g. Require frequent and unannounced security checks of barracks by unit officers and SNCOs.

h. Conduct briefings for incoming personnel concerning theft prevention.

i. Ensure personnel make prompt notification of stolen property to the Cherry Point Police.

j. Appoint responsible personnel as security managers for each barracks. Refer to reference (a) for instructions.

k. Establish a command objective of achieving a realistic reduction in barracks' thefts within a specified period. Considering the fact that most barracks thefts are crimes of opportunity, effects to reduce opportunity should produce a proportionate decrease in thefts.

l. Establish a key control program to ensure accountability of all keys for the barracks in accordance with reference (a). All spare room keys are to be maintained in a GSA approved metal key container. The key container will be secured to the building structure.

2. Government Owned Vehicle Security

a. Government vehicles will be secured with a locking mechanism when vehicles are parked and not attended by an assigned operator or crewmember. Exceptions to this policy are:

(1) Vehicles actively employed in tactical exercises and field operations.

(2) Dispatched emergency, Cherry Point Police, or guard vehicles for brief periods when response time is critical to the successful performance of the operator's or crew's duties.

(3) Inoperable or unserviceable vehicles; however, they must be protected from unauthorized cannibalization.

(4) Vehicles without installed locking mechanisms under the continuous surveillance of a guard(s) or located in a secured area.

b. Vehicles with locking mechanisms will be secured as follows:

(1) Commercial type vehicles: Activate manufacturer installed door and ignition locking device.

(2) Tactical vehicles: Immobilize steering wheel with a chain and padlock as specified in TM 9-232-28010 and TM 9-232-27210.

(3) Other government vehicles that cannot be secured as indicated in paragraphs (a) and (b) above, but require locking and lack manufacturer installed locking devices: Secure by using a locally fabricated system. The system used by a self-propelled vehicle should, at minimum, immobilize the steering mechanism and preferably the clutch and/or brake as well.

c. Government vehicles, when not in use, will be parked in motor pools or adjacent the building of assigned unit. Encourage personnel to park in well-lit areas wherever practical. A fenced-in area is preferable.

d. Roving guard personnel will perform a security check at least twice within a 24-hour period.

e. Accessible and easily removed components vulnerable to theft because of their value (radios, optical equipment, etc.) or utility (hand tools, basic issue items, etc.) will be provided additional security. Additional security for these types of components is essential when a vehicle is unattended and not under the protection of a dedicated guard and may be provided by:

(1) Storing in a secured structure.

(2) Storing in a locked, enclosed truck, van or vehicle trunk.

(3) Storing in a locked equipment box or similar container secured to an open bed vehicle; e.g., in a locked ammunition tool box chained to the bed of a 2-½ ton truck.

(4) Securing items directly to the vehicle by locally fabricated method.

f. Privately owned vehicles will not be allowed to enter motor pools.

g. Items that can be used to defeat security measures, such as bolt cutters, hacksaws, axes, steel rods or bars will not be left in the motor pool area unsecured. Tools of this nature will be secured in respective tool kits or in other secure areas such as a tool room when not in use.

h. Use of common key (master key) operated lock sets to secure government vehicles is prohibited. Keys and locks will be strictly controlled and accounted for in accordance with reference (a).

3. Hand Tools, Tool Sets, Kits, and Shop Equipment Security

a. Tool sets and kits with lockable tool boxes, when not in use, will be secured with a key operated, tumbler type padlock. The individual signed for the tools or kit will maintain possession of the key. A duplicate key may be maintained by the shop supervisor provided it is stored in a secure key container with controlled access.

b. When portable hand tools, tool sets or kits, and shop equipment are not in use or not under surveillance of a responsible person (user, supervisor, tool room keeper, guard), they will be stored in a secure location. Non-portable items are adequately secure in the building or vehicle in which they are located provided the doors and windows are closed and locked. Secure locations for portable items include:

(1) A locked building, room, or metal cage in a secure building.

(2) A locked built-in-cabinet, bin, or drawer in a room or building.

(3) Furniture items with a locked drawer or compartment (wall locker, desk, etc.) in a room or building.

(4) Attached to the building structure by use of a cable, chain and padlock, or permanently fastened to the floor or work surface; e.g. running a chain through the handles of a locked tool box and locking to a heavy pipe, or bolting light electric grinders to the work bench and peening or spot welding bolts to prevent easy removal.

(5) In locally fabricated lockable racks, when locked, that prevents the tool box lid for being opened or keep larger tools from being removed.

(6) In a locked enclosed truck, van, or vehicle trunk.

(7) In a locked vehicle equipment box or secured in a locked container secured to the vehicle itself; e.g., securing a tool box to the "eye" in the vehicle bed with a chain and padlock through the handles.

(8) Secured in a locked CONEX container.

c. Common tools and portable shop equipment not signed out on receipts or sub-signed receipts to a user will be controlled through a locally reproduced receipt, sign in/sign out log, or an exchangeable tag (chit) system. Tool checks, metal discs that can be stamped with the mechanics name or identification are available through the supply system under an NSN number in the 9900 group and class.

d. Access to tools and shop equipment will be controlled to the maximum extent possible. Access will be limited to user(s), the individual designated as responsible for security of items when not in use (tool room keeper, supervisors or command personnel).

e. Keys and locks used to secure hand tools, tool sets or kits, shop equipment and the facilities in which they are maintained will be controlled. Common keying (master key) lock sets will not be used to secure tools and shop equipment in accordance with reference (a).

f. Highly expensive and pilferable hand tools which have a non-military application and subject to theft and improper use will be placed under special control in SERVMART stores.

g. Consolidate tool storage within a facility or the unit shall appoint a tool room keeper to control the issuance and recovery of all tools.

h. Color code all tools and tool boxes with a paint stripe or mark to rapidly identify component parts of sets or kits. Tape may be used.

i. Use a display identification system to rapidly identify missing tools. Silhouette backdrops and plastic are two methods. Stencil control numbers on each tool box and the corresponding storage area when the tool box is not in use.

j. Conspicuously paint all shop equipment, in whole or part, a particular color or a particular pattern to discourage thefts and to assist in identification.

k. Permanently mark all tools and shop equipment by stamping, engraving, or scratching.

l. Prohibit removal of tools and shop equipment from work areas without specific authorization.

m. Closely monitor all tool losses and control pickups at the supply source to reduce opportunities for illegal diversions.

4. Administrative, Housekeeping Supplies, and Equipment Security

a. Furniture and Mess Equipment

(1) Work rooms in which these items are located or stored will be secured when no responsible member permanently assigned to that particular activity is present. Minimum security will consist of all doors and windows closed and locked.

(2) Furniture located in a recreation room or similar common area primarily used during the non-duty hours and not normally staffed, will be protected by controlling access to these areas to the maximum extent practical. This may be accomplished by requiring an individual who desires to use the facility to sign for the key(s) or having the duty officer or NCO periodically check the facility.

(3) Occupants of quarters will be responsible for the security of government furniture located therein.

(4) Mark the property with an identifier. This practice is particularly helpful in controlling items without serial numbers.

(5) Provide additional security for television sets, stereos, and other items vulnerable to theft by securing the items to the building structure with a chain or cable and padlock, or by enclosing the items in a locally fabricated metal cage.

(6) Maintain a record of the locations of items within the organization. The record should provide a brief description of the items, serial numbers, model numbers, and unit

identifiers, and rooms where items are located.

b. Office Machines/Government Electronics/Computers

(1) Buildings, rooms, and offices in which office machines are located will be secured whenever an individual permanently assigned to the activity, that occupies the room or office, is not present. Minimum security will consist of closing and locking all doors and windows.

(2) When size and weight allows, small office machines (laptops/cell phones, cameras, etc.) will be further secured by locking them in a desk or cabinet.

(3) Record all model and serial/asset numbers for identification purposes.

(4) Conduct a weekly inventory of all office equipment. Any missing equipment will immediately be reported to PMO.

(5) The responsible officer who signed for the equipment will constantly be aware of its location and status.

(6) Maintain a record of the location of items within their organization. The record should provide a brief description of the items, serial numbers, model numbers, unit identifiers, and rooms where the items are located.

c. Expendable/Consumable Supplies

(1) At the unit and office level, items not issued for actual use will be stored in a secure room, container, or building with access to keys and the storage facility strictly controlled.

(2) Pilferable items will be stored and issued from a security area such as a cage or a lockable closet or room. The manager will designate those items subject to abuse through excessive damage or consumption.

(3) Units and departments should establish consumption "norms" to provide a basis of future comparison for a parallel period of time. Periodic reviews should reveal trends, substantial changes, and appreciable differences in consumption among like units or offices that bear investigations.

(4) Use inspections to ensure units and offices retain adequate quantities of supplies to meet short term needs only. Excessive quantities of supplies are subject to pilferage.

5. Security of Subsistence Items

a. Subsistence storage facilities and refrigeration units will be secured at all times when entrances or exits are not under surveillance of personnel permanently assigned to the facility. Government key-operated, tumbler type padlocks will be used for this purpose except when a commercially installed locking device exists.

b. Keys and padlocks used to protect food items and subsistence storage facilities will be stringently controlled in accordance with reference (a).

c. Introduction of personal packages into and out of ration breakdown and subsistence storage areas will be restricted.

d. Access to ration storage areas will be strictly controlled. Access will only be authorized for individuals conducting official business.

e. All shipping containers, cases, etc. will be inspected to ensure they are empty and cardboard containers will be flattened prior to disposal.

f. Parking privately owned vehicles in the rear of the dining facility is prohibited after normal working hours.

g. Any signs of tampering will be immediately reported to PMO.

6. Repair Parts Security

a. Unit or department repair parts stock will be stored in a single area, readily accessible to maintenance or supply personnel to the maximum extent possible.

b. Portable repair parts will be secured by one of the following means:

(1) In a locked, separate building or room.

(2) In a locked, steel cage.

(3) In a locked built-in storage container (bin, drawer, cabinet) or a free standing container large and heavy enough to be non-portable with stored parts (desk, wall locker, CONEX box, etc.).

(4) To the building in which located or other permanent structure.

c. Non-portable repair parts will be secured by storing them in a building with doors and windows and secured during hours the facility is non-operational. When bulky or heavy items are stored outside, they will be protected by appropriate security measures.

d. Access to repair parts and parts storage areas, to include keys and padlocks protecting these items, will be stringently controlled in accordance with reference (a).

e. Require all used parts to be turned in. Ensure used parts are properly protected and disposed of to preclude unauthorized "recycling."

f. Spot check completed work to make certain new parts were installed and not switched with parts brought in from the outside.

g. Develop a system for recording identification of the individuals who receive and use the part(s).

h. Segregate all pilferable items and secure them in a separate room, building, or container with access limited to an appointed custodian.

7. Petroleum, Oil, and Lubricant (POL) Security

a. All fuel storage tanks and fuel issue points between 500 and 999 gallons will be designated, in writing, as Level I Restricted Areas. All fuel storage tanks and fuel issue points 1,000 gallons and greater will be designated, in writing, as Level II Restricted Areas.

b. POL tank trucks that contain fuel and are not under the surveillance of the operator will be secured as follows:

(1) Lock all hatch covers.

(2) Lock manifold access door.

(3) Secure each manifold valve with a transportation seal if a manifold access door cannot be locked.

c. Fuel pods on vehicles will be secured with padlocks when the vehicles or tanks are carrying fuel and are not under surveillance of the operator.

d. Fuel carrying vehicles will be parked in well lighted areas, in motor pools protected by locked perimeter barriers, or under guard whenever feasible.

e. Packaged POL products not onboard a vehicle will be safe guarded by one of the following means:

(1) In a structure capable of being secured.

(2) In an area protected by guards during the hours the storage facility is non-operational.

f. Ensure containers that can be used to carry fuel and hoses that can be used for siphoning are secured and not left lying around.

g. Place seals on all points of bulk fuel tanks, tank trucks, fuel pads, storage buildings, and containers that might allow extraction of fuel by any means. This practice is particularly important on points where padlocks cannot be used. Broken seals provide indications of tampering.

h. Monitor unit or department's usage to determine if it is excessive. Periodically validate unit or activity requirements against POL point of issue for indication of criminal activity. Spot check frequently and quantities of issue to specific vehicles at POL points against vehicle mileage for indications of pilferage or illegal use.

i. Spot check the contents of containers where used POL products are stored and ensure they are used (not fresh products) and properly marked. Ensure used POL products are stored separately. Supervise the loading of used products to ensure fresh stock is not being included with material being disposed of.

j. Ensure large POL packages, e.g., 55 gallon drums, are handled in such a way as to prevent their use as hiding places for pilfered items.

k. Prohibit entry of privately owned vehicles into military vehicle POL dispensing points.

l. Control circulation of commercial POL tankers on station. Cherry Point Police will check commercial tanker operators for possession of delivery order or copy of the procurement contract that authorizes them to enter the installation.

m. Follow-up on bulk POL issues to ensure that the quantity issued actually arrives at the destination. Seals and locks on tanks may also be used to guard against diversion en route.

n. Place locking gas caps on vehicles or install anti-siphon devices in vehicles to prevent thefts of POL products.

o. Review delivery and issue documents for indications of falsification (modification, fictitious aircraft or vehicle identification numbers of units, fictitious or dual delivery receipts, or forged documents).

Crime Prevention Programs Supplement

1. Use and Control of Protective Seals

a. Purpose of Seal. The purpose of the seal is to show whether integrity of a storage facility, vehicle or rail shipment, or container has been compromised. A plain seal is not a lock, although combination items referred to as "seal locks" are available. The whole purpose of a seal, no matter how well constructed, is defeated if accountability is not maintained.

b. Seal construction specifications should include:

(1) Durability. Seals should be strong enough to prevent breakage during normal use.

(2) Design. Seals should be sufficiently complex to make unauthorized manufacture of replacement seal difficult.

(3) Tamper Proof. Seals should readily provide visible evidence of tampering and be constructed in a way that makes simulated locking difficult once the seal has been broken.

(4) Individually Identifiable. Seals should have embossed serial numbers and owner identification.

c. Seal Security. Seals not issued for use should always be secured in a locked metal container with controlled access. Preferably, only Access Control Officers and custodians should have access.

d. Accounting of Seals

(1) Seal custodians should maintain seal accountability using bound log books instead of loose leaf binders.

(2) When seals are issued to a using office, unit or activity, the custodian will log the date of issue, name of recipient, and seal serial numbers.

(3) Units and departments will reflect seal numbers. All seals will be verified with a seal log, shipping documents, or other appropriate documents before removal and disposal. Seals should be deformed sufficiently upon removal so that they cannot be used to simulate a good seal. They may be disposed of in

normal trash.

(4) Colors of seals procured should be changed periodically as an additional physical security measure.

2. Key and Lock Control

a. Access Control Officer. All units/commands will appoint in writing a unit Access Control Officer and Access Control Custodian. The duties of these billets will include developing and implementing written procedures for the issuance/receiving of keys, maintain accountability and inventory of keys as required, ensuring the annual rotation of locks, changing of combination lock combinations, and other tasks as required by reference (a). The Access Control Custodian should have an alternate designated in writing to receive, issue, and account for keys in the absence of the Access Control Custodian.

b. Key Control Register. Keys will be signed out to authorize personnel, as needed, on a key control register. All personnel authorized to sign for keys will be assigned in writing. The key control register will, at a minimum, contain the identification number of the key, date and hour of issuance, signature of recipient and initials of individual receiving the returned key. When not in use, the key control register will be locked in a secure container with controlled access.

c. Key Depository

(1) A lockable container, such as a safe or filing cabinet, or a key depository made out of 26-gauge steel, equipped with a tumbler type locking device, and permanently mounted to a wall or structure, will be utilized to secure keys.

(2) Only necessary primary keys will be maintained in the depository for accountability. Duplicate keys will be stored in a separate locked container.

(3) The key depository will be locked at all times, except to issue or return a key to the conduct inventories.

(4) The key depository will be located in a room where it is under constant surveillance or in a room that can be secured during non-duty hours.

(5) All keys to AA&E storage containers or areas will be stored in accordance with reference (a).

(6) Keys to restricted areas will not be duplicated.

(7) At no time will keys to restricted areas be removed from the installation.

d. Locks

(1) U. S. Government key operated, tumbler type padlocks will be used to safeguard unclassified, non-sensitive supplies and equipment if a lock is required. The following padlocks are recommended. Selection should be based on value of items to be protected, operational requirements, and vulnerability to criminal attacks.

(a) Padlock, low security, key.

(b) Padlock, medium security, key.

(2) Master key (common key) padlock sets will not be used.

(3) Padlocks in use, offering a comparable level of security, should not be changed solely to conform to this enclosure.

(4) Padlocks not in use will be secured in a locked container along with their keys. Access to the container will be controlled.

e. Key and Lock Accountability

(1) Keys to locks currently in use protecting property of an office, unit or activity will be checked at the end of each duty day. Differences between on-hand keys and the key control register will be reconciled. Keys may be issued for personal retention if daily turn-in clearly jeopardizes mission readiness or seriously affects operational efficiency. Personally retained keys will be inventoried on a "show basis" at least monthly.

(2) Per reference (a), padlocks and their keys will be inventoried by serial numbers no less than semiannually. Daily sight counts of keys regularly issued are encouraged.

(3) Padlocks will be rotated at least annually. Rotation of existing locks and keys should be centralized and controlled by the key control custodian.

(4) When a key to a padlock is determined to be missing, the padlock will be replaced immediately.

f. Chains. When a chain is required for security of classified, non-sensitive equipment and supplies, it can be obtained through SERVMART or local sources.

3. Operation ID

a. Purpose of Markings. If properly done, marking of individual items of property serves three purposes:

(1) It acts as a deterrent to prevent theft or pilferage of items.

(2) It makes disposal of the property more difficult for the thief or pilferer (at pawn shops, for resale) since markings are not easily removed.

(3) It increases the chance for successful recovery of the property and prosecution of the perpetrator. Good markings allow police or investigators to prove more readily a loss to the government, track a specific item, and build a case against the thief or pilferer.

b. Determining When to Mark Items. This decision ultimately rests with the unit commander or department head, and property owner, since marking is not required. In making this judgment, the commander should conduct a vulnerability analysis and consider the costs associated with the marking effort. Markings should be considered particularly for items procured for military use from civilian manufacturers without modification in appearance and also available on the commercial market (same coloration, configuration).

c. Developing a Marking System. Marking is worthwhile only if it identifies a specific item as belonging to a particular organization. In the case of non-consumable items, marking makes a particular item unique as compared to other like items in the organization. Commanders and supervisors will determine the specific marking system that meets the needs of their organization. As a general rule, the marking system adopted should:

(1) Begin with a "US" or "USMC" to identify the item (to local pawnbrokers and other potential buyers) as Marine Corps property.

(2) Have a unit identifier. The identifier may be an abbreviation of the office, unit, or activity designation, a unit identification code, a code keyed to hand receipt or hand receipt line number, or any other combination of characters (letters, numerals, symbols) distinctive for the using organization.

d. Location of Markings on Items. Large, distinct markings serve the purpose of deterrence and are appropriate for items such as shop equipment where appearance is not important. Similar markings may be more desirable beneath desks for esthetic reasons. For high value items, such as televisions and stereos, an engraved plate attached to the front, with strong bonding cement, may act as a deterrent and not detract from the appearance of the item.

e. Ways of Marking Items

(1) Applying Decals. "Property of the United States Government" decals are available through GSA. Decals are primarily intended for office furniture and equipment.

(2) Paint Markings on Larger Items. Stencils are available through GSA under "Stencil Set Marking."

(3) Scratching or Scoring Markings on Metal Items. A diamond tip marking instrument, similar to a pencil, can be obtained through GSA. Order Scriber, Diamond Point.

(4) Etching or Stamping Metal Items. Various types of etching machines are available through standard supply channels.

f. Recording Marked Items. Records of marked items, including a brief item description, serial and model number, and name of individual to whom hand receipted, preferably the user, should be retained on file. These files should be kept at a location separate from the marked items, if possible. The files should be in a secure container with restricted access. Information should be made available to law enforcement personnel as soon as an item is determined missing, or if a loss cannot be explained, or a theft is suspected. Property inventory forms are available at the Physical Security Office, Building 251, Pass & ID, during normal working hours.

4. Recommended Public Relations Tools

a. McGruff the Crime Dog. The McGruff the Crime Dog campaign uses a costumed character and his partner, Officer Friendly, to deliver a message that, "The police cannot stop crime alone," and encourage community involvement.

b. Red Ribbon Week. National Family Partnership, formerly the National Federation of Parents for Drug Free Youth, was established as a grassroots, nonprofit organization in 1980 by a handful of concerned and determined parents who were convinced they should begin to play a leadership role in drug prevention. Their mission is to lead and support our nation's families and communities in nurturing the full potential of healthy, drug free youth.

c. National Night Out. National Night Out is an annual community-building campaign that promotes police-community partnerships and neighborhood camaraderie to make our neighborhoods safer, better places to live.

Physical Security Working Group Supplement

1. Information. Reference (a) requires the establishment of a Physical Security Council and Crime Prevention Council. In an effort to reduce the number of meetings with subjects that are closely related, the two councils will be briefed as the Physical Security Working Group (PSWG) in the Mission Assurance Working Group (MAWG) time slot.

2. Discussion. Reference (a) specifies that Crime Prevention and Physical Security are a command responsibility. However, it is through a total coordinated effort between commanders, staff agencies, and unit personnel that the best results in security effectiveness and crime prevention/reduction can be achieved. To be effective, a Physical Security Program must receive command attention and direction from all echelons within the chain of command.

3. Objectives. The objectives and goals of the MCAS Cherry Point PSWG are:

a. Coordinate and implement initiatives which support the installation's Physical Security and Crime Prevention Program.

b. Provide the Commanding Officer with a ready means for evaluating the effectiveness of all physical security measures and the crime prevention program.

c. Ensure that tenant commands develop physical security plans that complement the overall installation physical security effort.

d. Ensure that the installation physical security plan is fully integrated into and compliments the installation Mission Assurance Order and regulations.

4. Functions. The functions of the PSWG are:

a. Evaluate and prioritize physical security deficiencies for all restricted areas and critical infrastructures and provide courses for corrective action to the MAWG.

b. Evaluate crime trends or significant crimes or losses of property and levy specific tasks on commanders, officers-in-charge, or directors to support installation crime prevention efforts.

c. Recommend appropriate crime prevention measures.

5. Organization. The MA PM will serve as the chairperson for the MAWG, which encompasses the PSWG. The Physical Security representative to the MAWG will serve as the lead coordinator for PSWG requirements within the group. The functions of the PSWG require decisions to be made when meetings are conducted; therefore, appointments will be made that ensure continuity of attendance and the ability to represent unit/activity commanders. Listed below are the sections that will sit on the PSWG:

- Mission Assurance Program Manager - Chairperson
- Antiterrorism Officer - ATO
- Critical Infrastructure Program Manager - CIP
- CBRNE Protection Officer - CPO
- Installation Emergency Manager - IEM
- cPhysical Security - PSWG Office of Primary Responsibility

a. MAWG staff designated representatives as required:

- Airfield Operations (AirOps)
- Center for Naval Aviation Technical Training, Marine Unit (CNATTMARU)
- Combat Logistics Company-21 (CLC-21)
- Comptroller
- Defense Commissary Agency (DECA)
- Facilities Directorate (FAC)
- Fire Department
- Fleet Readiness Center-East (FRC-EAST)
- Joint Public Affairs Office (JPAO)
- Marine Corps Community Services (MCCS)
- U.S. Naval Health Clinic, Cherry Point (NHCCP)
- Naval Criminal Investigative Service (NCIS)
- Provost Marshal's Office (PMO)
- Safety and Standardization (SS)
- Staff Judge Advocate (SJA)
- Station Veterinarian
- Logistics Directorate (LOG)
- Telecommunication Information Systems Directorate (TISD)
- Marine Transport Squadron-One (VMR-1)
- Second Marine Aircraft Wing (2d MAW)

6. Administration. The Physical Security Working Group will meet quarterly in accordance with reference (h). A PMO Physical Security representative will coordinate with the Mission Assurance Program Manager to schedule and upload the Physical Security PowerPoint at the end of the MAWG brief. Minutes of the meeting will be recorded by Mission Assurance and distributed to the Commanding Officers and members of the council.

Unit Letter Head

5530
UNIT CODE
DD MMM YY

From: Commanding Officer, Appropriate Unit
To: Provost Marshal, (Attn: Physical Security)

Subj: REQUEST FOR MARINE CORPS ELECTRONIC SECURITY SYSTEM

Ref: (a) MCO 5530.14A

Encl: (1) Diagram of Building/Area (OPTIONAL)

1. Per the reference, (Unit) requests that a MCESS intrusion detection system (IDS) be installed in Bldg. **XXX**, Room **XXX**. The installation of this intrusion detection system in this facility, Bldg. **XXX**, Room **XXX**, is to meet all physical security requirements for (open storage of classified material, storage of AA&E).

2. (Unit) is aware of and understands that it will be responsible for all required funding incurred for this IDS installation project.

3. If there are any questions or concerns for this matter, please contact (POC) at (252) 466-XXXX.

J. D. JONES

Unit Letter Head

5530
UNIT CODE
DD MMM YY

From: Commanding Officer, Appropriate Unit
To: Provost Marshal, (Attn: Physical Security)

Subj: REQUEST FOR PIN ISSUANCE FOR (BUILDING/AREA)

Ref: (a) MCO 5530.14A

Encl: (1) Diagram of Building/Area (OPTIONAL)

1. Per the reference, request that a MCESS PIN be issued for (Room/Building/Area/Door) to the below listed personnel.

NAME	RANK/BILLET	DOD EDI#

2. If there are any questions or concerns for this matter, please contact (POC) at (252) 466-XXXX.

J. D. JONES