COMSCINST 5530.4	COG CODE N15	DATE 15 MAY 1995

DEPARTMENT OF THE NAVY
COMMANDER MILITARY SEALIFT COMMAND
WASHINGTON NAVY YARD BLDG 210
901 M STREET SE
WASHINGTON DC 20398-5540

COMSCINST 5530.4
N1
15 May 1995

COMSC INSTRUCTION 5530.4

Subj: PHYSICAL SECURITY PLAN

Ref: (a) OPNAVINST 5530.14B
(b) SECNAVINST 5500.4G
(c) OPNAVINST 5510.1H
(d) OPNAVINST 5239.1A
(e) NDW Notice 5520 of 2 Dec 87
(f) NDWINST 5520.1
(g) OPNAVINST 3140.24E
(h) N1 Memo N12/JPW/aec 003241 of 20 Oct 92

1. Purpose. To provide guidelines and procedures for implementing physical security measures at Headquarters, Military Sealift Command (MSC) and to define specific actions required to safeguard personnel, equipment (including Automated Information Systems (AIS) assets), facilities, material and documents from unauthorized access such as espionage, sabotage, theft or other unlawful acts.

2. Mission. The mission of the Military Sealift Command (MSC) is to meet Department of Defense requirements by providing efficient sea transportation, combat-ready logistics forces and reliable special mission ships in peace and war.

3. Responsibilities. Commander, MSC is responsible for ensuring that appropriate measures are taken to safeguard personnel and property within the command; establishing and maintaining a formal physical security program and acting as final authority in determining the type and extent of physical security protection required for the facility.

4. Applicability. This instruction is applicable to all military and civilian personnel assigned to or employed/located at Headquarters MSC and MSC Central Technical Activity (MSCCENTACT).

C. R. BURCHELL
Deputy Commander

Distribution:
COMSCINST 5000.19
List I (Case A, B)
List II (Case A, B)

TABLE OF CONTENTS

Chapter 6 - Security Force

Chapter 7 - Terrorist Threat Conditions

APPENDICES

RECORD OF CHANGES

The Military Sealift Security Plan will be kept current by the issuance of changes which will be incorporated upon receipt. A record of such changes will be recorded in the space provided below.

CHANGE NO.	DATE OF CHANGE	DATE ENTERED	SIGNATURE

CHAPTER 1

SECURITY OFFICE STAFFING AND FUNCTIONS

1-1 STAFFING

Director, Military Personnel and Security Division (N15) serves as the Security Officer at MSC and comes under the cognizance of the Director, Personnel, Manpower and Management (N1). The MSC Security Officer is responsible for supervising two security specialists, GS-080-7 through 12, who implement the command's Physical Security Plan. The security specialists work as a team in performing duties in personnel, information and physical security while maintaining liaison with various Naval and DOD activities.

1-2 SECURITY OFFICER

The Security Officer, either personally or through subordinates is responsible for the following:

a. Implementing, administrating, training and overseeing a comprehensive security program consistent with command guidelines and those established by higher authority. Serves as the command representative for security matters.

b. Designing and developing protection systems and devices to ensure that the material and facilities are not compromised, sabotaged, subjected to malicious mischief or other forms of willful interference.

c. Identifying restricted areas, setting up personnel access systems; developing procedures for the movement and handling of classified and other sensitive materials.

d. Preparing correspondence, reports and directives.

e. Formulating emergency plans; maintaining liaison and personal contact with ADP Security Officer, Federal agents and NDW Security Department.

f. Accomplishing other related duties as specified in reference (a).

1-3 SECURITY CLERK/SECURITY SPECIALIST

The security specialists work independently under the supervision of the MSC Security Officer in performing the following duties:

a. Developing and entering data in buildings 210 and 157 computerized access systems.

b. Conducting physical security surveys for buildings 210 and 157.

c. Supervising random security inspections.

d. Overseeing and/or assisting in emergency evacuations, as required, from buildings 210 and/or 157.

e. Supervising and providing guidance to contract security guard personnel in buildings 210 and 157.

f. Physically changing security combinations to all of command security containers and maintaining an inventory of containers.

g. Initiating Report of Surveys and maintaining computer database for periodic reports.

h. Maintaining liaison with the Naval District Washington (NDW) Security Officer regarding various security policies, security related incidents and activities.

I. Providing authorization letters/memoranda to employees and contract personnel for an NDW security badge after verification of requirement or approval from MSC sponsor and receipt of current visit request.

j. Producing and maintaining buildings 210 and 157 contract guard force post orders.

k. Overseeing the command Intrusion Detection systems located in Strategic Analysis Subsystem (SEASTRAT) (2nd floor of building 210) and WWMCCS (Worldwide Military Command and Control System) Intercomputer Network Site (WINSITE) (3rd floor of building 210) spaces.

CHAPTER 2

SECURITY MEASURES

2-1 RESPONSIBILITIES

a. Security Officer. The Security Officer is responsible for planning, coordinating and supervising the command's Physical Security Program. Included in the program are the following:

(1) All matters pertaining to physical security.

(2) Formulating Emergency Plans.

(3) Reviewing and updating the COMSC Physical Security Program.

(4) Complying with other related duties as specified in reference (a).

(5) Establishing and maintaining liaison with personnel or agencies to ensure timely and organized support in event of an emergency.

b. MSC military personnel and civilian employees will be responsible for adhering to the sound security practices set forth in this plan and become familiar with evacuation procedures used during all emergency situations.

2-2 MATERIAL CONTROL

a. General. MSC Physical Security and Loss Prevention Program is designed to safeguard resources from theft, vandalism or misappropriation by establishing an unacceptable risk of detection and/or apprehension. Reference (a) provides more detailed guidance.

(1) Accountability. Personnel taking government equipment (e.g., lap top computers, typewriters, recorders, etc.) out of building 210 and 157, will have a property pass from a designated N4 representative or a letter of authorization signed by a designated N6 representative. Memoranda and property passes will be in duplicate; the original to be retained on file and the duplicate to be retained by the bearer. Buildings 210 and 157 security guard post orders identify the designated N6 personnel authorized to sign the letter of authorization.

(2) Reporting Losses. Loss of government property should be reported immediately to the MSC Security Officer who will notify NDW Security Department and the local Navy Criminal Investigative Service (NCIS). NCIS will be the primary resource for detection and investigation of lost, stolen or missing government property. All government property, regardless of value or classification will be reported to this agency for stolen or recovered

property. Loss of personal property will be reported immediately to MSC Security Officer who will notify the NDW Security Department for action.

(3) Missing, Lost or Stolen Report (MLSR) Procedures. Missing, lost or stolen government property, including accidentally destroyed data, will be reported in accordance with current directives and accountable individuals will be identified by N4. Property inventories will be matched with existing property. Investigations will be submitted with loss reports. Detailed instructions for MLSR reporting requirements and the proper message format can be found in reference (b). The Security Officer is the focal point for tracking MLSR reports.

(4) Administrative Inspections. COMSC is responsible for readiness, security, health, welfare and safety of members of this command and those members of other commands who use MSC property. A notice will be posted in buildings 210 and 157 advising that all handcarried items, such as briefcases, bags, boxes, etc., will be subject to random security inspections prior to entrance or departure. The inspections will be directed by the Commander and the procedures listed below will be followed:

(a) The inspection shall be specifically authorized in writing by COMSC or his designee.

(b) A member of the MSC Security Office will be present and in charge.

(c) Personnel will be stopped randomly without regard to status (i.e., civilian employees, contractor, military personnel or visitors). Individuals will be selected with a random numbering system outlined by the Commander or Designee's signed authorization.

(d) Security Guards will explain to the personnel stopped that an inspection is being conducted. The individual will be asked to step out of the walk way and to open his/her briefcase, purse, etc. for inspection. If an individual entering refuses to do this, he or she will be prohibited from entering the spaces and no inspection will be conducted. For those leaving, the inspection will still be done even after objection of the party and if necessary the Security Officer will notify NDW Security Department. Otherwise, the individual will be allowed to proceed after inspection.

b. Physical Security Review Committee (PSRC)

(1) General. COMSC has overall responsibility for physical security and law enforcement matters affecting MSC buildings 210 and 157. COMSC will establish the Physical Security Review Committee (PSRC) which will include the Chief of Staff (N001) as chairperson.

(2) The PSRC will meet in accordance with reference (a) and perform the following:

(a) Assist in determining physical security requirements for and evaluating security areas at MSC.

(b) Advise on establishment of restricted areas.

(c) Review draft physical security and loss prevention plans or recommend changes prior to submission to COMSC.

(d) Review reports of significant losses or breaches of security and recommend improvements to the Physical Security and Loss Prevention Program.

(3) The PSRC membership will include the following staff members:

(a) Chief of Staff (N001) (Chairperson)

(b) Security Officer (N15)

(c) Personnel Officer (N1)

(d) Logistics Director (N4)

(e) Inspector General (N00I)

(f) ADP Security Officer (N61)

c. Security Officer. Under the direction of COMSC, the Security Officer is responsible for the establishment, administration and coordination of physical security and law enforcement measures involving the protection of military personnel and civilian employees. Inclusive in these responsibilities is the implementation of the Loss Prevention Program. The Security Officer will ensure the program is properly established and administered and will make periodic reports on its progress to COMSC. He or she will maintain close liaison with the NDW Security Department to ensure proper compliance in the Loss Prevention Program and to provide input for revisions to the plan.

d. Directors/Special Assistants. Each Director/Special Assistant is responsible for the security of personal property, equipment and spaces assigned to that directorate or members of that directorate. Directors/Special Assistants will maintain close liaison with the MSC Security Officer regarding Physical Security and Loss Prevention and ensure proper compliance with the command's program.

2-3 INTERNAL CLASSIFIED DOCUMENT CONTROL PROCEDURES

a. Security Manager. The Security Manager is responsible for planning, coordinating and supervising the Information and Personnel Security Program.

b. Control Information. Effective control of the Department of Defense (DOD) information will be maintained at all times in accordance with reference (c). All classified material received at MSC must be brought into the mailroom accountability system. Secret or Confidential classified material received through mail or any other means of transmission will immediately be handcarried to the mailroom for entry into the classified material accountability system. Top

Secret or NATO classified material received by mail or any other means of transmission will immediately be handcarried to the TS/NATO Classified Material Control Officer who is assigned to N6. TS/NATO classified material is not handled by mailroom personnel or entered into the mailroom classified material accountability system.

c. Storage. All classified documents, when not in use, will be stored in a GSA-approved security container. MSC Security will maintain an inventory of all security containers, the locations, custodians and record of combination changes. The SDO is provided a listing which includes the location of each container and that listing will be used for the daily MSC security checks.

(1) Combinations to the security containers must be changed at least once annually, when an individual knowing the combination no longer requires access, when the combination has been subject to possible compromise, when the security container has been discovered unlocked or unattended, when the container is first put into service or when the security container has been taken out of service.

(2) Combination changing tools are maintained by the MSC Security Office and are available for use by authorized MSC employees to change combinations to MSC security containers. The custodian must advise the MSC Security Office when one of the above listed occurrences have come into effect and at that time set up an appointment with a MSC security specialist for changing the combination. When scheduling the appointment, ensure that the custodian of the security container is present and available during the combination change.

(3) Combinations are not to be changed by individual employees unless approved by MSC Security Office in advance.

(4) Security containers will be repaired by an approved contract locksmith with a facility clearance. Repair requests will be approved by the MSC Security Office and coordinated with N4.

d. Destruction. Classified documents that are no longer required are to be immediately destroyed using a GSA-approved shredding machine located in buildings 210 and 157 as follows:

(1) **Building 210**
- (a) Room 352
- (b) Room 334
- (c) Room 449
- (d) Room 404
- (e) Room 425
- (f) Room 456
- (g) Room 306
- (h) Room 217
- (i) Room 234
- (j) Room 136
- (k) Room 131

(2) **Building 157**

(a) Room 304
(b) Room 406
(c) Copy room

e. Emergency Removal. MSC shall develop an emergency plan to protect classified material in a manner that will minimize the risk of injury or loss to personnel. If removal of classified material from building 210 or 157 is not feasible, the material shall be stored in a GSA approved container.

2-4 PERSONNEL IDENTIFICATION REQUIREMENTS

a. Because buildings 210 and 157 are restricted areas, one of the following forms of identification badges are approved before unescorted entrance to the buildings:

(1) Naval District Washington (NDW) identification with "MSC" stamped in bold red letters on the front of the badge.

(2) NDW contractor identification badge with "MSC" stamped in bold red letters on the back of the badge.

(3) National Capital Region (NCR)/Pentagon (PNT) badge with pink, red and/or white backgrounds.

(4) MSCLANT Bayonne, NJ, MSCPAC Oakland, CA, MSCFE Yokohama, JA, MSCEUR London, UK

(5) National Defense Executive Reserve (NDER)

(6) Armed Forces of the United States with badges in green, red or blue.

(7) United States Transportation Command.

b. Personnel requesting entry to buildings 210 and 157 to perform maintenance or contract services will be positively identified prior to allowing entry. A current visit request must be on file in the MSC Security Office on those individuals in order to be listed in the computer access system. The visit request can be either a letter from the agency on company letterhead or a form listing the individual's full name (last name and first name), social security number, date and place of birth, citizenship, purpose of visit, name of MSC point of contact and length of visit (not more than 1 year). The correspondence must be signed by a security representative or a designated agency representative.

c. Individuals who request entry and cannot produce required identification media, and/or are not on the access list, will be denied entry until they are personally escorted/accompanied by a staff member when in buildings 210 and 157.

2-5 PERSONNEL SECURITY CLEARANCE AND ACCESS REQUIREMENTS

Before contractors and visitors at MSC are granted access to classified information, clearance eligibility must by verified by the MSC Security Office. Contractors and visitors must ensure that a visit request is forwarded by mail or fax to the MSC Security Office prior to their visit. Visit requests will not be accepted if hand delivered by an individual whose name is on the visit request. The information provided in the visit request must be in compliance with reference (c). Clearance eligibility on employees will be verified by MSC through the Department of the Navy (DON) Central Adjudication Facility and Human Resources Office (HRO) record center. A security clearance access list is provided to directorate heads at least monthly and at that time supervisors will review and make requests for changes as required.

2-6 BARRICADED CAPTOR/HOSTAGE SITUATIONS

MSC will comply with the procedures delineated in reference (f) concerning these situations as applicable.

2-7 THREAT CONDITIONS

MSC shall comply with applicable threat requirements outlined in reference (a).

2-8 BOMB THREAT/DETECTION PROCEDURES

Personnel will comply with procedures outlined in COMSCINST 3440.3E.

2-9 DESTRUCTIVE WEATHER

MSC will follow the procedures outlined in reference (g) when destructive weather threatens. Snow emergency procedures are described in reference (h).

2-10 FIRE EVACUATION PLAN

In the event of fire comply with the procedures outlined in COMSCINST 3440.3E.

2-11 KEY AND LOCK CONTROL

a. Responsibilities

(1) Commander. Responsible for establishment of the Key Control Program within the command and appointment of a key control custodian.

(2) Key Control Custodian. Responsible for the command's overall key control program as outlined in reference (i). Keys to the command Restricted Areas are maintained in locked key cabinets and security containers located in the MSC Security Office. Administrative keys are maintained by the Logistics Director in a locked key cabinet. Keys are issued only to those persons approved by the Security Officer (staff personnel only). The Key control custodian is required to perform spot checks and inventory all keys at least quarterly.

(3) Security Officer. Designated the Key Control Officer for MSC. Responsible to the Commander for all security related key control and lock control functions at MSC.

(4) Director/Special Assistants. Responsible for ensuring that the key control program is implemented within their codes. He or she must notify N4 whenever a key is lost/stolen or when an employee departs the command before returning keys; for restricted area keys N15 must be notified in writing. Directors/Special Assistants will request duplication of keys through N4.

b. Key Control Log

(1) A Key Control Log will be maintained with each key locker and when not in use will be kept under constant control of the custodian. When no personnel are available to oversee the log, it will be secured in an area qualified to hold classified material. The log will contain information to include keys issued, to whom, date/time issued and returned and the signature of the person drawing or returning the key. The control log will be checked against the key at the end of each watch or work period to account for all keys and an appropriate notation will be made in the Command Duty Log. There are only two classified key lockers in the command. They are located in the Command Control Center (CCC), which is manned 24 hours a day, and the Security Office. The key locker in the Security Office is stored in a security container and maintained by a Security Specialist. None of these keys are reissued.

(2) Included within the key inventory are all keys, locks, padlocks and locking devices used to protect or secure restricted areas and activity perimeters, critical assets, classified material and sensitive materials and supplies. Not included in the inventory are keys, locks and padlocks for convenience, privacy and administrative or personal use.

(3) There will be no more than two duplicate/spare keys kept onhand. Duplicates will at no time be checked out to personnel for convenience. Before a duplicate key is checked out, the key custodian will establish the need for the duplicate and the disposition of the original. All requirements for duplicate keys will be routed through the key custodian to the command security office. A record of keys replaced will be kept in the key control log for future reference and review.

c. After Hours Procedures. Keys are maintained in the Command Control Center (CCC). The SDO has custody of the keys which can be used to access all spaces (non-restricted including maintenance and restricted areas in buildings 210/157). Each of the keys are labeled and a log is maintained by the SDO who will use these keys for the duty sections to make the security checks for buildings 210 and 157 daily.

2-12 PROTECTIVE LIGHTING

Continuous lighting at both entrances to Building 210 and 157 illuminates the vehicle parking area and provides assistance to the NDW Security Police in preventing illegal intrusion attempts.

2-13 COMMUNICATION

Classified information will not be discussed over non-secure telephones or in non-secure spaces.

2-14 AUTOMATED DATA PROCESSING SECURITY OFFICER (ADPSO)

The ADPSO will ensure command ADP equipment is operated in accordance with reference (d).

CHAPTER 3

CONTROL MEASURES

3-1 CONTROL MEASURES (RESTRICTED AREA)

This chapter identifies all mission essential areas within MSC. Building 210 is designated as a restricted area. All persons are forbidden to enter established restricted areas unless their official duties require such entry. As a restricted area, there are procedures for conducting administrative inspections of persons entering and leaving such areas. The purpose is to detect/prevent the introduction of prohibited items (firearms, explosives, drugs, etc.) and to detect/prevent unauthorized removal of government property/material. Administrative inspections should be conducted on a random basis daily, but at least monthly. The inspections shall be specifically authorized in writing by COMSC or his/her designatee, the MSC Security Officer. Security guards will conduct the inspections with a member of the MSC Security Office present and in charge during the inspections.

3-2 AREA SECURITY

Areas, offices and other structures at MSC which are designated as restricted fall into one of the following categories:

a. Level Three Areas. A Level Three restricted area is the most secure type of restricted area. It may be within less secure types of restricted areas. Entrance procedures for all Level Three restricted areas include an access list of personnel authorized to enter area without an escort. The access list will include name and rate/rank of each individual permitted uncontrolled access. Requirements for Level Three areas are as follows:

(1) Personnel identification and control system (i.e., activity area pass/ID or military/civilian government identification card) must be displayed at all times on the outer garment. During normal duty hours, use of an access list and entry/departure log is required. After normal duty hours, all personnel accessing the area must be logged in/out.

(2) Only persons whose duties require access and who have been granted appropriate security authorization will be admitted to Level Three areas. Persons who have not been cleared for access to the security interest contained with a Level Three area may be admitted, but they must be controlled by an escort, and the security interest protected from compromise or other degradation.

(3) When secured, a check will be made at least twice every 8 hour shift or, if adequately equipped with an operational IDS, once per 8 hour shift, for signs of unauthorized entry or other activity which threatens to degrade security of the Level Three restricted area.

b. Level Two Areas. Buildings 210 and 157 have no Level Two areas.

c. Level One Areas

(1) Persons authorized to enter Level One areas are those assigned duties requiring their presence while actively engaged in performing such duties.

(2) A Level One restricted area is the least secure type of restricted area and serves as a buffer zone for Levels Three and Two restricted areas providing administrative control. The following minimum security measures are required for all Level One restricted areas.

(a) A personnel identification and control system.

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

(c) Procedures to control entry into the area by individuals (military, civil service, contractors, official business, individuals who render a service (e.g., vendors, delivery people, designated contractors performing a service, etc.)) retired military and unofficial visitors.

d. Non-Restricted Areas. A non-restricted area is an area which is under the jurisdiction of MSC but to which access is minimally controlled or uncontrolled. Such an area may be open to uncontrolled movement of the entire command or the area can be enclosed by a check point which would ensure access for official business or other authorized purpose only. Non-restricted areas will not be located inside restricted areas. All areas not designated as Restricted Areas are designated as non-restricted areas at MSC.

e. Posting of Restricted Areas. Restricted areas within MSC buildings will be posted simply as "Restricted Area." Posting of signs will be in accordance with paragraphs 0307 of reference (a).

f. Movement Control within Security Areas. Security personnel will have full cooperation and participation of other military and civilian personnel. All personnel in security areas will be instructed to consider each unidentified or improperly identified individual as a trespasser and report him/her to their supervisor, the Security Officer or to other appropriate authority.

g. Personnel Identification and Control Procedures. Buildings 210 and 157 are restricted areas; therefore, entry will be granted only to authorized personnel. Security guards will verify the identity of all personnel before entry to MSC buildings 210 and 157. Personnel must provide a current picture badge and/or be on the automated access system before entry. Personnel and visitors will comply with procedures as described below.

(1) MSC military and civilian employees with the following authorized badges are not required to sign in the log book.

(a) NDW identification badge with "MSC" stamped in bold red letters on the front of badge. Reference (e) outlines NDW badge policies.

(b) NCR/PNT badge (pink, red and/or white)

(c) MSC Area Command picture badges

1. MSCLANT Bayonne NJ

2. MSCPAC Oakland CA

3. MSCFE Yokohama, JA

4. MSCEUR London, UK

(d) NDW contractor identification badge with "MSC" stamped in bold red letters on the back of badge.

(2) Visitors with badges listed below are authorized access to buildings 210 and 157 but must sign in the visitor log. Exceptions to this rule are also listed below.

(a) National Defense Executive Reserve (NDER)

(b) Armed Forces of the United States (military identification cards -- green, red or blue colored)

1. Military members who are not in access control system must sign the visitor log.

2. Military members who are not in access control system must be escorted. (This does not include command suite visitors.)

3. Military, civilian or visitors who are on access system will be provided the following internal badges prior to verifying their identity. Individuals must sign in/out visitor log prior to being provided a badge.

a. "T" badge will be given military or civilian employees who forget their MSC picture or NCR/PNT badge.

b. "V" badge will be given to federal government or contractors.

(3) All other visitors who are not on the MSC access system will be given a "Visitor with Escort" badge and those visitors must be escorted at all times. The security guard will also contact the point of contact to request an escort for the visitor.

(4) Command Suite/VIP Visitors. The security guard will be notified prior to any visits to the command suite (N00, N01 and N02). Visitors will be escorted by someone in the command suite. (No sign in log book is required). The following procedures will be followed:

(a) Security guard will be notified by the command suite (N00, N01 and N02), prior to any visits to the command suite.

(b) Security guard will contact command suite when visitor arrives.

(c) Visitor will be escorted by someone in the command suite.

(d) Visitor will not be required to show identification, the escort from the command suite will verify identity of visitor.

(5) Weekend Drilling Reservists. U.S. Navy Reservists who perform weekend drills and meet at COMSC Headquarters, will ensure that a list is provided periodically to the MSC Security Office prior to their visit. The following procedures will be followed by the security guards in buildings 210 and 157.

(a) Check the military identification of the reservist.

(b) Check the access list for the individual's name.

(c) Ensure that reservist signs in/out log.

(d) If the name is in the access system and the reservist holds an NDW/MSC badge, they are not required to be issued a "V", "T", or "Visitor with escort badge."

(e) If name is not in access system, issue reservist a "V" badge.

(6) After Hours Procedures. All persons entering or leaving building 210 on weekdays during the hours between 1900 (7:00pm) and 0500 (5:00am) will sign in/out log book. No one will leave through building 157 after 1800 (6:00pm). All personnel who are located in building 157 after that time will leave through building 210.

(a) All personnel will sign in regular visitor log on weekends and on holidays.

(b) Deliveries made after hours, weekends and/or holidays shall be left at the guard desk. Security guards are to notify SDO of package and make a note in the log books.

(7) Law Enforcement. The security guards shall cooperate with Federal, State, County and local law enforcement officials who visit MSC in an official capacity. The official will present their credentials to the security guard and after verification of their identity MSC security office will be notified immediately during regular working hours or the SDO after hours and on weekends and holidays.

(8) Agents of Investigative Agencies. For all Federal Bureau of Investigation (FBI), Naval Criminal Investigative Service (NCIS), Defense Investigative Service (DIS), U.S. Treasury Department, Secret Service or Office of Personnel Management (OPM) investigative personnel requesting admittance to buildings 210 or 157 the procedures below will be followed:

(a) Credentials will be checked;

(b) MSC Security Office will be notified during normal hours; after hours, the SDO will be notified.

CHAPTER 4

MATERIAL CONTROL

4-1 PROPERTY CONTROL PROCEDURES

Reference (a) requires the controlled movement of government property. The use of property passes is essential to external security and loss prevention. Every precaution must be exercised to ensure the integrity of government material.

a. Property Pass (NAVSUP 155). This form authorizes removal of certain specifically described government or private property from MSC through control points. It is the standard form to be used by MSC when appropriate documentation showing proof of ownership or authorization for possession is not with the government or private property. Other proof of ownership or authorized documentation is:

(1) Government bills of lading

(2) Commercial bills of lading

(3) Adding machine tape annotated "SERVMART COMSC" used for all SERVMART purchases

(4) DOD Single Line Item Release/Receipt Document (DD Form 1348-1)

(5) Requisition and Invoice/Shipping Document (DD Form 1149)

(6) Blanket Purchase Authorization (BPA) (NSC 4225/1)

(7) Subsistence Report Multi-use (NAVSUP 1059)

(8) Material Inspection and Receiving Report (DD 250)

b. Property Passes

(1) A property pass, issued by N4, will accompany government property from MSC through Buildings 210 and 157 guard force.

(2) Property passes will be picked up by the guard force in either Building 210 or 157.

(3) The guard force/security official will review the property pass for authenticity of the signature or entries for documentation or where serial numbers are not annotated on the property pass.

4-2 RESPONSIBILITIES

a. The Logistics Director (N4) shall:

(1) Maintain accountability and control over MSC property passes.

(2) Obtain an adequate on-hand supply of property passes and ensure that they are stored in combination lock containers.

(3) Appoint a directorate custodian to obtain and maintain accountability of property passbooks (including disposition of originals) and return completed passbooks to the Security Officer. Information regarding any suspected usage irregularities in property passes shall be reported to the Security Officer.

(4) List items/property being removed from building 210 and/or 157 and record serial numbers for each item on property pass. Also record dates of issue, signatures and duty stations of persons to whom issued and keep for control purposes.

b. Security Officer shall:

(1) Review MSC property passes returned. Send copy to Property Manager (N41a) to update property control system.

(2) Inspect completed passbooks received from N4 to ensure all returned passes have been matched with the duplicate copy and each missing original has been accounted for by the issuing directorate. Investigate all matters indicating possible misuse, fraudulent changes or any other irregularities. Directors/ Special Assistants and N4 will be advised of any discrepancies and will be requested to take corrective action.

(3) Periodically review the use and application of property passes and ensure they are being properly utilized.

(4) Establish and maintain liaison between NDW Security and other appropriate officials to ensure property passes issued by MSC are returned to this command.

4-3 INFORMATION MATERIAL CONTROL

Control of classified and Privacy Act information/material is addressed in reference (c). The Security Manager is responsible for the information and personnel security program; the ADP Security Officer (ADPSO) is responsible for the ADP security program.

CHAPTER 5

PHYSICAL SECURITY AIDS

5-1 SECURITY LIGHTING

DOD security personnel are responsible for the inspection of security lighting, while maintenance comes under the jurisdiction of the Public Works Department.

a. Protective Lighting. Protective lighting is utilized around the perimeter areas of Buildings 210 and 157 as a means of security illumination for workers entering and departing during hours of darkness.

b. Auxiliary Lighting. Generators and power source will be considered for critical areas. Back-up generators are located in building 210 and specifically for the Communications Center in Building 210 only.

5-2 POWER FAILURE PROCEDURES

a. In the event of a commercial power failure during regular work hours, NDW Public Works Department will be notified by COMSC (N4) or the contract security guard.

b. After regular work hours, NDW Security Department and NDW Public Works Department will be notified by Building 210 security guard or by the MSC SDO.

5-3 INTRUSION DETECTION SYSTEM (IDS)

a. IDS is designed to detect, not prevent, actual or attempted penetrations. IDS contributes to the overall physical security posture and the attainment of security objectives. The IDS systems are located in the SEASTRAT and WINSITE spaces. When the IDS system alarm sounds, the contract security guards in building 210 will respond by calling the MSC Security Office during normal work hours and after hours by calling NDW Security Police or the MSC SDO. In the event of power failure, the Security Guard will notify the SDO who will check both spaces to ensure there have been no successful attempts to gain entry to the spaces.

b. The following personnel at MSC are responsible for ensuring that the IDS is maintained.

(1) Commander, MSC has overall responsibility for the proper installation and hook-up of all alarms in buildings 210 and 157 including the designated spaces/areas.

(2) The Security Officer (N15) and the Logistics Director (N4) must approve all systems prior to hook-up to ensure compatibility.

(3) The MSC Security Officer will provide and monitor the alarm system in MSC buildings 210 and 157.

CHAPTER 6

SECURITY FORCE

6-1 GENERAL

One contract security guard is assigned to building 210 and one guard is assigned to building 157. These security guards will be issued special orders which cover specific situations pertaining to that specific post. Each security guard reporting for duty will review the post orders and become familiar with its contents at the beginning of his/her watch. At the end of each watch the security guard will brief the oncoming security guard of any changes to the post orders or any significant special incidents. The guard orders will be reviewed at least semiannually by the MSC Security Officer.

6-2 RESPONSIBILITIES

The armed security guards at MSC Headquarters and MSC Central Technical Activity (MSCCENTACT) are located at the entrances of building 210 and 157 will perform the following duties at the above listed posts:

a. Control the entry and exit of all personnel, equipment and property.

b. Protect U.S. government property and employees and visitors.

c. Maintain all of the guard logs/registers in a neat and legible manner.

d. Keep constantly alert and observe everything within sight or hearing.

e. Report all violations of published and/or verbal orders.

f. Remain on assignment until properly relieved by direction of contract guard supervisor.

g. Pass all information relative to assignment to the relieving guard.

h. Turn over any money or valuables recovered to MSC Security Officer.

i. Endeavor to prevent theft, pilferage, riots, espionage, sabotage and other criminal acts.

j. When directed, conduct random security inspections of incoming/outgoing personnel, briefcases, purses, packages, etc.

k. Ensure that all personnel bringing and removing government and/or agency property have a valid property pass (if necessary) and sign the property log book.

l. Ensure that prohibited material such as firearms, explosives, drugs, etc. does not enter the building.

m. Issue appropriate "V", "T", "Visitor with Escort" and "Distinguished Visitor" badges to visitors or employees. Ensure that none of these badges leave buildings 210 and 157.

n. Be professional and courteous in all situations.

o. Apprehend and detain persons only within their jurisdiction and then only for as long as necessary to transfer such persons to NDW Police. MSC Security Officer will be notified from 0600 to 1630; the SDO will be notified from 1630 to 0600 on weekends and holidays regarding the situation.

6-3 SUPERVISION

Assigned security guards come under the direct supervision of the NDW Contracting Office with the COMSC Headquarters Security Officer providing daily guidance in carrying out assigned duties. Changes to these instructions will normally come from the COMSC Security Officer. However, between the hours of 1630 and 0600 weekdays and all day Saturday, Sunday and holidays, the authority to modify orders is given to the COMSC Staff Duty Officer (SDO).

6-4 METHODS OF FORCE

The minimum amount of necessary force shall be used in all situations. The methods and instruments are listed from the least severe to the most severe and the following applies:

a. Physical apprehension and restraint techniques, e.g., come-along holds.

b. Standard issue security devices, not including firearms, i.e., the baton. The baton may be used in the following situations:

(1) To subdue a resisting subject in self-defense or in protection of a third party.

(2) As a blocking or repelling device in crowd control.

(3) To ward off blows from an assailant.

c. Firearms may be drawn and readied for use in situations where it is anticipated that they may be actually required.

(1) In accordance with the Naval District Washington Security Directive 24-90, the minimum amount of force shall always be used by the security guard force.

(2) The use of deadly force (the drawing of or actual use of a weapon) is the **last resort** measure and the contract security guards will do so only in the following situations.

(a) Self defense. When deadly force reasonably appears to be necessary to protect security personnel, military, civilian, contractors and or visitors in buildings 210 and 157 from death or serious bodily harm.

(b) Serious offense. When deadly force appears to be necessary to prevent a serious offense involving violence and threatening death or serious bodily harm (such as arson, armed robbery, aggravated assault or rape).

(c) Lawful Order. In addition to normal superior authority, a "Lawful Order" to fire a weapon on post may be given by the following MSC personnel:

1. Commander, MSC

2. Vice Commander, MSC

3. Deputy Commander, MSC

4. Chief of Staff, MSC

5. Security Officer, MSC

6. Staff Duty Officer (SDO), MSC

NOTE: There is a picture of the Commander and Vice Commander posted at each guard post for verification. The SDO will present a badge to indicate that he/she is the duty officer.

6-5 PRECAUTIONS FOR USE OF DEADLY FORCE

Before the use of deadly force, the following precautions shall be taken to prevent possible death or serious bodily harm.

a. An order to halt shall be given before firing a shot.

b. Shots shall not be fired if it is likely that an innocent bystander may be harmed.

c. Warning shots may not be employed because it constitutes a hazard to innocent persons.

d. Only authorized issued firearms and ammunition shall be carried and used by the contract security guards in the performance of their duties and during training.

e. A discharge of firearms, other than during authorized training, or any instance of misuse or mishandling by guards shall be reported immediately to the MSC Security Officer, the NDW Security Officer, and the NDW Contracting Officer.

6-6 EMERGENCY PROCEDURES

a. During emergencies (fire alarm, medical emergency, evacuation, etc.) emergency personnel will be permitted immediate entry. Contract security guard will immediately call the MSC Security Officer during normal hours or the SDO if after normal work hours, weekends and/or holidays and advise them of the situation.

b. In case of fire or natural disaster, the security guard in building 210 or 157 will immediately notify the following as applicable:

(1) Fire Department 433-3333

(2) Ambulance 433-3269

(3) NDW Security Dept 433-3017/3211

(4) SDO 685-5155 (1630 - 0600)

(5) MSC Security Officer 685-5144/5145/5146
(0600 - 1630)

CHAPTER 7

TERRORIST THREAT CONDITIONS (THREATCONs)

7-1 INTRODUCTION

Information and warnings of terrorist activity against MSC and attached personnel will normally be received from security authorities or through security agencies. Information may come from NDW Police Department, be received directly by command or agency as a threat or warning from a terrorist organization or be in the form of an attack.

7-2 DECLARATION OF TERRORIST THREATCONs AND MEASURES FOR IMPLEMENTATION

The declaration of THREATCONs and implementation of measures may be decreed by the Commander, MSC, following receipt of intelligence through official sources, the Naval District of Washington, other official channels or following an anonymous threat message. Actions should be based on all appropriate sources of information to include intelligence, law enforcement and knowledge of the location situation. Reference (a) provides detailed THREATCON procedures.

7-3 THREAT ASSESSMENT GUIDELINES

a. General Guidelines. The following general guidelines provide for uniform implementation of security alert conditions. Assessment factors are defined as follows:

(1) Existence. A terrorist group is present, or able to gain access to a given building.

(2) Capability. The acquired, assessed or demonstrated level of capability to conduct terrorist attacks.

(3) Intentions. Recent demonstrated anti-U.S. terrorist activity or assessed intent to conduct such activity.

(4) Targeting. Current credible information on activities indicative of preparations for specific terrorist operations.

(5) Security Environment. The internal political and security considerations that impact on the capability of terrorist elements to carry out their intentions.

b. Threat Levels. Threat levels are based on the degree to which combinations of the following factors are present:

(1) Critical. Factors of existence, capability and targeting must be present. History and intentions may or may not be present.

(2) High. Factors of existence, capability, history and intentions must be present.

(3) Medium. Factors of existence, capability, history and must be present. Intentions may or may not be present.

(4) Low. Existence and capability must be present. History may or may not be present.

(5) Negligible. Existence and/or capability may or may not be present.

7-4 VULNERABILITIES

The following are MSC vulnerabilities:

a. Communication lines and support facilities

b. Power supply transmission (primary and alternate)

c. Logistic and storage facilities

d. Computer facilities - access to LAN or individual "stand alone" microcomputers

e. Intrusion detection system monitor station

f. Water sources

g. Personnel

(1) Flag officers/senior civilians

(2) Foreign personnel assigned to or visiting the command

7-5 THREAT CONDITIONS

a. THREATCON ALPHA. This condition is declared as a general warning of possible terrorist activity, the nature and extent of which is unpredictable, when the circumstances do not justify full implementation of the measures of THREATCON BRAVO. However, it may be necessary to implement selected measures from THREATCON BRAVO. The measures in this threat condition must be capable of being maintained indefinitely.

b. THREATCON BRAVO. This condition is declared when there is an increased and more predictable threat of terrorist activity even though no particular target is identified. The measures of this threat condition must be capable of being maintained for weeks without causing undue

hardship, without affecting operational capability and without aggravating relations with local authorities.

c. THREATCON CHARLIE. When an incident occurs or when intelligence is received indicating that some form of terrorist action against installations or personnel is imminent. Implementation of this measure for more than short periods will probably create hardship and will affect peacetime activities of the installation and its personnel.

d. THREATCON DELTA. A terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally this THREATCON is declared as a localized warning.

APPENDIX A

SECURITY SERVICING AGREEMENT

NOTE: MSC Security Servicing Agreement will be separate from the MSC Physical Security Plan.

APPENDIX B

INDEX

SUBJECT **PARAGRAPH**