



DEPARTMENT OF THE NAVY
FLEET AVIATION SPECIALIZED OPERATIONAL
TRAINING GROUP PACIFIC FLEET

NAS NORTH ISLAND
SAN DIEGO, CALIFORNIA 92135-5122

FASOTRAGRUPACINST 5530.1C CH-1

10

20 AUG 1990

FASOTRAGRUPAC INSTRUCTION 5530.1C CHANGE TRANSMITTAL 1

Subj: PHYSICAL SECURITY AND LOSS PREVENTION PLAN

Purpose. To promulgate change 1 to the basic instruction

2. Action. Make the following changes to the basic instruction.

a. Change reference (b) to read "NASNIINST 5530.3A"

b. Delete reference (g).

c. Where appearing, change "reference (g)" to read reference (b)".

d. Reletter "references (h) through (l)" to read "(g) through (k)" and change accordingly where appearing.

3. Cancellation. Upon completion of required action.

A handwritten signature in black ink, appearing to read "D. E. Ballard", is written over a light-colored rectangular stamp or background.

D. E. BALLARD

Distribution:

FASOTRAGRUPACINST 5216.2R

Lists A and B



DEPARTMENT OF THE NAVY
FLEET AVIATION SPECIALIZED OPERATIONAL
TRAINING GROUP PACIFIC FLEET

NAS NORTH ISLAND
SAN DIEGO, CALIFORNIA 92135-5122

FASOTRAGRUPACINST 5530.1C

10

27 FEB 1990

FASOTRAGRUPAC INSTRUCTION 5530.1C

PHYSICAL SECURITY AND LOSS PREVENTION PLAN

- (a) OPNAVINST 5530.14B
- (b) NASNIINST 5530.3
- (c) COMNAVAIRPACINST 5530.3
- (d) OPNAVINST 5510.1
- (e) FASOTRAGRUPACINST 5530.2
- (f) OPNAVINST 5290.1
- (g) NASNIIST 5510.15
- (h) SECNAVINST 5500.4
- (i) FASOTRAGRUPACINST 4500.1
- (j) NASNIINST 5512.6
- (k) NASNIINST 5512.5
- (l) NASNIINST 5100.37

- (1) FASOTRAGRUPAC Restricted Areas
- (2) Security Badge/Access Control Procedures
- (3) Physical Security of Classified Material
- (4) Key Control and Accountability Procedures
- (5) Physical Security of Audio-Visual/Minor Training Devices
- (6) Bomb Threat Procedures
- (7) Loss Prevention Program
- (8) Crisis Response Procedures
- (9) Terrorist Procedures
- (10) Hostage Bill
- (11) Fire Bill
- (12) Physical Security Review Committee/Board
- (13) Inter/Intra Service Support Agreement
- (14) Security Education and Training
- (15) Material Control
- (16) Protective Lighting

1. Purpose. To establish procedures to protect Navy property and personnel at FASOTRAGRUPAC using procedures contained in enclosures (1) through (16) and in accordance with references (a) through (l).

2. Cancellation. FASOTRAGRUPACINST 5530.1B. Changes in this instruction are extensive as to require a complete review. Revisions, additions and deletions have not been specifically identified.

3. Background. Physical security is that portion of the overall security program concerned with physical measures designed to safeguard personnel, prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against espionage, sabotage, terrorism, damage, and theft. The physical security program is concerned with means and measures designed to safeguard personnel and protect property by preventing, detecting, and

FASOTRAGRUPACINST 5530.1C

27 FEB 1990

confronting acts of unauthorized access, sabotage, wrongful destruction, malicious damage, theft, pilferage, and other acts which would reduce to some degree the capability of the command to perform its mission.

4. Responsibilities. Security is the direct, immediate, and moral responsibility of all military and civilian personnel employed by the Department of the Navy. To that end:

a. The Commanding Officer is responsible for the physical security and loss prevention program within the command.

b. The Security Officer, designated by letter, is the Commanding Officer's direct representative responsible for planning, implementing, enforcing and supervising the physical security and loss prevention programs of the command. This individual shall be an E-7 or above who has attended the Shore Based Physical Security Officer course.

5. Applicability. This instruction is applicable to all military and civilian personnel located/employed at this command.

6. Scope. This instruction applies to Buildings 646, 618, 707 and 502. Remote Training Site Warner Springs is covered by a separate instruction.



D. E. BALLARD

Distribution:

FASOTRAGRUPACINST 5216.2Q

List A and B

27 FEB 1990

FASOTRAGRUPAC RESTRICTED AREAS

The second deck of Building 707 is designated as a Level Two Restricted Area. In accordance with reference (a), the following minimum security measures are required:

1. A clearly defined and protected perimeter. The point of ingress will be clearly posted with the following:

WARNING
RESTRICTED AREA - KEEP OUT
AUTHORIZED PERSONNEL ONLY

IT IS UNLAWFUL TO ENTER THIS AREA WITHOUT
THE PERMISSION OF THE COMMANDING OFFICER. ALL
PERSONNEL AND PROPERTY UNDER THEIR CONTROL
WITHIN THIS RESTRICTED AREA ARE SUBJECT TO SEARCH.

2. A personnel identification and control system in accordance with enclosure (2) of the instruction.

3. Ingress and egress to these spaces will be controlled by the established Code 32 watch personnel and all spaces will be secured during non-working hours

4. Admission only to persons whose duties require access and who have been granted appropriate authorization. Persons not cleared for access to the security interests contained therein may, with appropriate approval, be admitted, but they must be controlled by a cleared Code 32 escort at all times, and the security interests protected from compromise.

5. When secured, checked at least twice per 8-hour shift by the NAS North Island Security Force. The NASNI Security Force will check for signs of attempted or successful unauthorized entry to Bldg. 707, and for other activity which could degrade the security of the Level Two Restricted Area.

Encl (1)

27 FEB 1990

SECURITY BADGE/ACCESS CONTROL PROCEDURES

1. GENERAL. Headquarters staff and student personnel, official visitors, and other non-staff personnel shall wear identification badges while on the second deck of Bldg 707. Badging is designed to promote physical security by providing the basis for early identification of unauthorized personnel. This badging program applies to all military, civilian, contract personnel, and visitors. Staff badges will be issued by the Classified Files Clerk in Bldg 646. Student/visitor badges will be issued by Code 32 personnel.

2. DUTIES AND RESPONSIBILITIES. To avoid physical security violation at this command, the following procedures shall be followed:

a. FASOTRAGRUPAC photo card badges will be worn by all personnel accessing Code 32 spaces (second deck Bldg. 707).

b. A clip or chain will be used to affix the badge face out at or above the waist of the individual.

c. FASOTRAGRUPAC badges will be issued to Code 32 staff personnel upon initial check-in. All other badges will be issued as required. (1) Blue colored badges will be issued to appropriate staff personnel; (2) yellow colored badges to student personnel; and (3) white colored badges to visitors.

d. All personnel are reminded of the following warning printed on the back of the badge: "Issued for official use of the holder designated hereon. Use or possession by any other person is unlawful and will make the offender liable to penalty."

3. CONTROL PROCEDURES

a. Staff personnel

(1) FASOTRAGRUPAC staff security badges (Blue) will be issued, upon initial check-in, only to AW personnel assigned to the staff. Exceptions to this rule will be authorized and granted by the Command Security Manager.

(2) Issuance and return of Staff Security Badges will be logged by the Classified Files Clerk in the Security Badge Log. (Members will sign the Security Badge Log acknowledging receipt of the Security Badge).

b. Student/Visitor personnel

(1) FASOTRAGRUPAC student (yellow) and visitor (white) security badges will be issued by Code 32 personnel.

(2) Students will be issued badges only after proper identification has been matched with a class roster. Students not found on class rosters must be cleared through the Department Security Petty Officer.

Encl (2)

27 FEB 1990

(3) Visitors will be issued badges after proper identification has been verified against the Security Access/Visitor Log. If this verification is not possible, the Department Security Petty Officer is to be notified for authorization.

(4) All visitors will be logged in/out in the Visitors Log.

(5) An escort will be provided for all visitors and such escort shall be present prior to allowing the visitor to enter the spaces.

c. Upon exiting the security area, security badges will always be returned to the security desk watch.

d. In the event a security badge is lost/missing, the Command Security Manager is to be notified immediately and will determine if a new badge is to be issued. A list of all lost/missing security badges will be maintained by the Code 32 security desk watch and the Command Security Manager. This list will be updated immediately upon notification of a lost/missing badge. All badges will be replaced after a loss of 6% of the badges or after 6 years, whichever comes first.

e. All security badges will be serially numbered according to classification, and badges on hand will be inventoried semi-annually in June and December. Inventory results will be forwarded to the Command Security Manager.

f. The printer's plates for badges will be safeguarded by the Command Security Manager. Unissued "blank" security badges will be protected in locked containers.

g. All personnel are charged with compliance and enforcement of badging procedures. It shall be each individuals responsibility in Code 32 to challenge unbadged personnel and report violations to the Command Security Manager immediately.

27 FEB 1990

PHYSICAL SECURITY OF CLASSIFIED MATERIAL

1. PURPOSE. Classified material or information may be used or discussed only where the facilities are adequate to prevent unauthorized persons from gaining access. The requirements in this enclosure represent the minimum acceptable standards which will allow for the accomplishment of essential functions while affording appropriate security.

2. RESPONSIBILITIES OF DEPARTMENT SECURITY CUSTODIANS

a. Department security custodians are responsible, at all times, for safeguarding classified material.

b. Stowing classified material in appropriate security containers whenever not in use or under the direct supervision of appropriately cleared personnel.

c. Ensure classified material is not discussed with or in the presence of unauthorized personnel.

3. SECURITY OF WORKING SPACES. Working spaces containing classified material will be afforded necessary measures to prevent unauthorized personnel from gaining access to material. Security measures will include those necessary to prevent unauthorized persons outside Bldgs. 618, 646 and 707 or within their spaces from viewing or hearing classified material or information. The ~~top~~ deck of Bldg. 707 is designated as a Level Two Restricted Area. ^{second}

4. SECURITY OF CLASSIFIED MATERIAL DURING WORKING HOURS

a. During working hours, precautions shall be taken to prevent access to classified information by unauthorized personnel.

b. Classified material will not be disclosed or released to personnel unless personnel are cleared to receive information and have a NEED TO KNOW.

c. Classified material cover sheets will be used on all classified material.

d. Classified documents, when removed from storage for working purposes, will be kept under constant surveillance and placed face down or covered when not in use.

e. Classified information/material will not be removed from officially designated offices or working areas for the purpose of working on such material during off duty hours.

f. Preliminary drafts, carbon sheets, notes, worksheets, and all similar items containing classified information will be destroyed by a method authorized for destroying classified material, immediately after they have served their purpose. If not destroyed, subject material will be safeguarded and assigned the same classification as the original information produced.

Encl (3)

27 FEB 1990

g. Typewriter ribbons used in typing classified material shall be protected in the same manner as required for the highest level of classification for which they have been used. They must be destroyed as classified waste.

5. SECURING OF CLASSIFIED MATERIAL

a. Department Security Custodians shall require a security check at the end of each working day, ensuring all classified material is properly secured. An Activity Security Checklist shall be used.

b. Ensure all classified material is stored in the manner prescribed by reference (d).

c. Burn bags will be used for disposal of classified material. Ensure they are properly stored or turned in for destruction.

d. Check and ensure contents of wastebaskets do not contain classified material.

e. Check and ensure containers/safes containing classified material have been locked by responsible personnel, rotating the dial of the combination lock in the same direction at least four complete times. Record on Security Container Check Sheet.

6. STORAGE OF CLASSIFIED MATERIAL

a. Valuables such as money, jewels, and precious metals shall not be stored or held in containers used to store classified material.

b. Classified material will not be stored in nonapproved filing cabinets, safes or desks.

c. Containers shall not have external markings which indicate the level of classified information stored within.

d. Each container and drawer holding classified material will be numbered

e. Index or inventory lists of classified material will not be posted on outside of safe or container, but will be kept inside the front of each drawer.

7. REPRODUCTION OF CLASSIFIED MATERIAL

a. Permission must be obtained from the Command Security Manager prior to reproducing Secret material. When approved, two people, where possible, will be involved in reproducing classified material.

b. Personnel reproducing Secret material will be responsible for ensuring proper control and handling procedures are enforced.

c. Designated reproducing machines shall be posted with the following sign: "THIS MACHINE MAY BE USED FOR REPRODUCTION OF MATERIAL UP TO SECRET. REPRODUCTION MUST BE APPROVED BY THE COMMAND SECURITY MANAGER." Appropriate warning notices prohibiting reproduction of classified material shall be posted on equipment authorized only for reproduction of unclassified material.

d. Reproduced copies of classified documents are subject to the same security control prescribed for the material from which the reproduction is made.

e. Samples, waste, or overruns resulting from the reproduction process shall be safeguarded according to the classification of the information involved and shall be destroyed promptly as classified waste.

f. Reproduction material shall show or be marked to show the classification and other special markings which appear on the original material from which copies were reproduced.

g. After reproducing classified material, two blank copies or a scramble sheet will be passed through the reproduction machine to ensure all classified images have been erased from the reproduction drum.

8. SAFE AND CONTAINER COMBINATIONS

a. Combinations will be changed under any of the following circumstances:

(1) When placed in use after procurement.

(2) Whenever an individual knowing the combination no longer requires access.

(3) When the combination was compromised or the security container or safe was discovered unlocked and unattended.

b. Copies of work requests for combination changes will be kept on file for two years.

c. Combinations of containers and safes will be assigned the security classification equal to the highest category of material stored in the container or safe.

d. Records of combinations will be sealed in an envelope, Security Container Information, and kept on file by the Classified Files Clerk.

9. EMERGENCY PLAN FOR CLASSIFIED MATERIAL

a. Each department handling classified information will develop and post an emergency plan for the protection of classified material.

b. The emergency plan, at a minimum will:

FASOTRAGRUPACINST 5530.1C

27 FEB 1990

(1) Include a listing of classified material by type, location, priorities for destruction, and the prescribed place and method of destruction, if required.

(2) State that, in the event of a fire, immediate evacuation of the building is of paramount importance, and that classified material is not required to be properly stored before leaving.

(3) Require that an inventory of classified material be made as soon as possible after the emergency to determine accountability and to report any compromises.

KEY CONTROL AND ACCOUNTABILITY PROCEDURES

1. PURPOSE. To establish a control and accountability system for FASOTRAGRUPAC office/building door keys, as required by references (a) and (e).

2. DISCUSSION

a. The need to strictly maintain the physical security of command offices/buildings is of paramount importance. As such, strict control and accountability of keys must be maintained. A loss of key accountability is a breach of security.

b. Included in the key and lock control program are all keys, locks, padlocks and locking devices used to protect or secure restricted areas, classified material, sensitive material and supplies. Keys, locks and padlocks used for convenience, privacy, unclassified administrative or personal use are not included in this program.

c. Keys may be classified into four categories: (1) Compartment keys - a single office or space; (2) Sub-master key - keys which allow access to several spaces or offices within a department; (3) Grand Master keys - keys which allow access to all offices or spaces with similar locks throughout the command; and (4) Building entry keys.

d. All keys described in subparagraph 2b require control and accountability. Compartment and Sub-master keys shall be centrally issued and controlled at the department level. Grand master and building entry keys shall be maintained in a locked key box in the Duty Office and will be controlled by the Key Control Officer.

e. Duplication of keys shall be strictly controlled and minimized. Only the Key Control Officer will authorize all key duplication requests. (Duplication of building entry keys, grand master keys, and sub-master keys is not authorized.)

3. RESPONSIBILITIES

a. The Security Officer will assume the responsibilities of the Key Control Officer, be designated as such in writing, and is directly responsible for all security-related key and lock control functions within the command.

b. Department Heads will designate, in writing, a key custodian who will be responsible to the Key Control Officer for all keys controlled by that department. Department Heads may, at their discretion, assign sub-custodians, as necessary. Key custodians will maintain a log book showing keys on hand, keys issued, to whom, date/time the keys were issued and returned, and the signatures of persons drawing or returning keys.

FASOTRAGRUPACINST 5530.1C
27 FEB 1990

c. Duplicate keys will be stored in a central key box located in the Command Duty Office (Bldg 646). These keys will only be issued by the OOD/AOOD and will be noted in the key log book upon issuance and return. The key box will be inventoried each working day at 0730 and a duty log book entry will be made. The Key Control Officer will be notified immediately of any discrepancies.

d. The Key Control Officer will conduct an annual inventory of all controlled issued keys in December and will maintain appropriate logs and records.

e. Department Key Custodians will inventory keys issued to custodial key log accounts quarterly in March, June, September and December. Inventories shall be retained for three years.

PHYSICAL SECURITY OF AUDIO-VISUAL/MINOR TRAINING DEVICES

1. All nonconsumable items are plant accounted when received by the Material/Supply Office. Custody cards are completed, signed by the department head, maintained by the Material/Supply Officer and inventoried annually. Duplicate custody cards are signed by the division supervisor and maintained by the department head.
2. Newly acquired audio-visual items are reported to COMNAVAIRSYSCOM in accordance with reference (f) and inventoried annually.
3. Highly pilfeable devices are stored in strong room with security lock and very limited access.
4. All documentation regarding equipment and media within the Media Department is computerized for ease of tracking and reporting.
5. All activities utilizing the FASO Aviation Training Aids Library (ATAL) system must designate in writing, by the Commanding Officer, personnel authorized to draw devices. Activities requiring semipermanent custody must designate a primary media custodian.
6. Primary media custodians are recommended to be the Supply/Material Officer for proper inventory control.
7. All activities are sent semi-annual inventories for all equipment checked out to their command. Inventories are signed, returned, and kept on file.
8. A semi-annual preventive maintenance system (PMS) requires all devices (except projection screens) to be returned for maintenance with a physical sight inventory and condition codes updated.
9. Activities that are more than 60 days overdue on any required inventory or maintenance schedule are automatically locked out by the computer system. No devices, or media can be checked out until required action is complete.
10. Full computer system access is strictly limited to provide positive control and tracking. The computer logs all transactions for all devices, media, and authorized users including the librarian that performed the transaction.
11. Activities missing or losing equipment on loan from FASO are required to report the loss immediately to the FASOTRAGRUPAC ATAL who will:
 - a. Release the initial Missing, Loss, Stolen Report (MLSR)
 - b. Send a message to the borrowing activity directing a JAG Manual Investigation, notify the Naval Investigative Service and next higher command.

27 FEB 1990

BOMB THREAT PROCEDURES

1. PURPOSE. To outline the course of action to be followed during periods of suspected, imminent, or in-progress bomb threats/incidents involving FASOTRAGRUPAC buildings.

2. DEFINITIONS

a. Bomb. A device capable of producing damage to material and injury or death to personnel when detonated or ignited.

b. Bomb Threat. A communication delivered by any means which may or may not specify the location of the bomb; include the time for detonation/ignition; or contain an ultimatum related to the detonation/ignition or concealment of the bomb.

c. Bomb Incident. Involves any occurrence concerning the detonation/ignition of a bomb, discovery of a bomb or receipt of a bomb threat.

3 Take the following actions during normal working hours:

a. Individuals Receiving Information Regarding a Bomb Threat shall:

(1) Remain as calm as possible and try to ascertain as much useful information from the caller as possible, i.e., when it will go off, where it is planted; what it looks like, why it's being planted, time of call, etc. The bomb threat checklist, Attachment (1), should be utilized.

(2) Immediately notify the CO, XO, and OOD so a decision can be made to evacuate the building, if necessary.

(3) Notify the NAS North Island OOD. The NASNI OOD will make notifications as required by reference (g).

(4) Initial OPREP-3 report will be made by the NASNI CDO. Subsequent reports will be released by FASOTRAGRUPAC.

(5) Department heads, as applicable, will:

(a) Upon receiving word to evacuate, ensure classified material and high value assets are properly secured, time permitting.

(b) Open all doors and windows.

(c) Instruct personnel to evacuate in an orderly manner via the nearest exit and proceed to an open area.

(6) When determined the bomb threat was a hoax or the explosives have been rendered safe by the EOD team, the CO/XO will make the decision to reopen the building(s).

Encl (6)

FASOTRAGRUPACINST 5530.1C

27 FEB 1990

4. Take the following procedures after normal working hours:

a. The AOOD receiving information of a bomb threat will immediately notify the OOD.

b. The OOD will:

- (1) Immediately notify the NASNI OOD.
- (2) Notify the CO and the XO.
- (3) Submit OPREP-3 reports, as applicable.

DEPARTMENT OF THE NAVY

TELEPHONIC THREAT COMPLAINT

IF BOMB THREAT, ASK THE CALLER

- WHEN IS THE BOMB TO GO OFF?
- WHERE IS THE BOMB TO GO OFF?
- WHAT KIND OF BOMB IS IT?
- WHAT DOES THE BOMB LOOK LIKE?
- WHERE ARE YOU CALLING FROM?

COMMAND

a. Name & Address

b. Phone No.

2. COMPLAINANT

a. Name

3. PERSON RECEIVING CALL

a. Name

b. Date & Place of Birth

c. Command Name & Address

d. Phone Number
(Work)

(Home)

4. TELEPHONE CALL RECEIVED ON

a. Phone Number (Include area code)

b. Location

c. Phone number listed in ("X" all that apply)

Command Directory

Base Directory

Local Directory

Unlisted

Other (list)

5. DETAILS OF CALL

Date

b. Day of Week

c. Time

6. CONTEXT OF CONVERSATION

a. Recipient "

b. Caller "

c. Recipient "

d. Caller "

e. Recipient "

f. Caller "

7. BACKGROUND NOISES (Describe street sounds, voices, music, etc. If more space is needed, continue on reverse.)

8. INFORMATION ABOUT CALLER/VOICE CHARACTERISTICS

a. Sex

b. Age

c. Race

d. Accent

e. Educational Level

f. Attitude (Calm, Nervous, Serious)

g. Other

WERE THERE ANY WITNESSES TO THE CALL?

No

Yes (List name)

10. DO YOU HAVE ANY SUSPICION AS TO THE IDENTITY OF THE CALLER?

No

Yes (List name)

11. NOTIFICATION OF AUTHORITY ("X" all notified)

- CO XO OOD Security NISRA Telephone Company EOD Fire Dept.

LOSS PREVENTION PROGRAM

1. PURPOSE. A vigorous loss prevention program is essential as loss of property may prevent the timely accomplishment of mission requirement and cost millions of dollars annually. Losses must be minimized by application of a comprehensive loss prevention program consisting of loss analysis, proper use of available investigative resources, continuing employee loss prevention education, application of firm corrective measures, administrative personnel action and pursuit of prosecution, and other loss prevention measures where necessary.

2. PREVENTION

a. Exterior doors and windows, storage rooms, and office buildings which contain high value, sensitive, or pilfeable property, supplies, or office equipment will be afforded security protection commensurate with the value and sensitivity of the contents.

b. At a minimum, hinges will either be non-removable or be provided with inside hinge protection, preventing locked doors from opening even if hinges are removed, and lock and hasp security systems that meet Military Specification (MILSPEC) Standards for the office's or room's contents.

3. EDUCATION

a. All employees (military and civilian) will be indoctrinated on procedures for preventing property losses as well as his/her responsibility for the care and protection of government property. This indoctrination will be included in the individuals initial security briefing and annually thereafter.

b. Loss prevention topics will also be included periodically in the POD.

4. PERSONNEL RESPONSIBILITY

a. Command procedures for the issue and control of government property must ensure strict accountability is established for individuals responsible for government property which is reported missing, lost, or stolen.

b. Recoupment action will be undertaken against an individual in each case where the individual's negligence or noncompliance with procedures, instructions or directives result in missing, lost or stolen government property which is a reportable loss.

c. Individuals accountable for government property will be held responsible for negligent loss.

5. CONTROL PROCEDURES

a. Office equipment will be marked with a serial number, entered on an inventory sheet, and, when not in use, stored to preclude pilferage.

FASOTRAGRUPACINST 5530.1C

27 FEB 1990

b. When office spaces are left unattended or during non-duty/working hours, doors will be secured and access controlled.

c. When possible, equipment will be secured or bolted to desk tops, etc. to prevent pilferage.

6. PILFERABLE OFFICE SUPPLIES (CONSUMABLE)

a. All office supplies subject to pilferage will be stored in locked cabinets when not needed.

b. Officer supervisors will monitor usage of consumables to ensure supplies are not being pilfered.

7. REPORTING. The guidelines for the reporting of missing, lost, stolen or recovered government property are contained in references (h) and (i).

27 FEB 1990

CRISIS RESPONSE PROCEDURES

DEFINITION. For this plan, crisis actions include, but are not limited to:

- a. Hostage situations
- b. Terrorist acts
- c. Civil disturbances
- d. Sabotage
- e. Natural disasters

2. Upon notification of a crisis situation(s) occurring onboard FASOTRAGRUPAC controlled spaces, the OOD will immediately notify the:

- a. Executive Officer
- b. NASNI Security Police
- c. NASNI Duty Officer

d. If appropriate, the department head having responsibility for spaces nearest the crisis situation location.

3. The OOD should be prepared to assist the On-Scene Commander for Crisis Response in the following:

- a. Evacuation of personnel from FASOTRAGRUPAC spaces.
- b. Providing names/telephone numbers of staff personnel required to assist.
- c. Identifying locations of classified/sensitive materials.

4. When crisis situation(s) involve FASOTRAGRUPAC spaces/personnel, the OOD shall:

- a. Maintain a chronological written record of events occurring during the crises.
- b. Prepare appropriate messages, when directed.

5. The OOD shall not:

- a. Conduct negotiations.
- b. Participate or cause any FASOTRAGRUPAC employee(s) (military or civilian) to become involved in any response/action effort(s).

Encl (8)

TERRORIST PROCEDURES

DEFINITIONS

a. Terrorism. The unlawful use or threatened use of force or violence against individuals or property, with the intention of coercing or intimidating governments or societies often for political, religious or geological purposes.

b. Acts of Terrorism. Acts of terrorism directed at naval personnel, activities or installations have the potential to destroy critical facilities, injure or kill personnel, impair or delay accomplishment of mission and cause incalculable damage through adverse publicity and public perception of incident handling and results.

2. TERRORIST METHODS. The record of terrorist activities directed at military activities indicate that the following methods might be employed:

a. Bombs. Bomb(s) used may be of any degree of sophistication and may be placed to destroy equipment, cause fires, create casualties, etc.

b. Ambush. Rapid ambush attacks by individuals or small groups to assassinate individuals or eliminate groups of naval personnel.

c. Armed Attack. An armed assault, usually with one or more diversionary actions, carried out by small groups against key personnel or critical assets with the objective of causing disruption of command mission and creating adverse publicity.

d. Hostage Situations. A terrorist group may undertake the seizure of specific hostage(s) for ransom, media attention, coercion or political bargaining purposes. Whenever possible, personnel should avoid situations which may lead to being taken hostage by terrorists.

3. THREAT CONDITION (THREATCON) DESCRIPTIONS. Terrorist THREATCONS designate the security posture to be established during periods of possible terrorist activities. Threat conditions will be established by COMNAVBASE San Diego as Area Coordinator to increase the formal level of anti-terrorist readiness and to upgrade physical security readiness. Procedures listed below will be followed during the different levels of THREATCONS.

a. THREATCON ALPHA. THREATCON Alpha will be implemented when a possible terrorist activity against military personnel or facilities in the San Diego area is predicted.

(1) Upon notification to implement THREATCON Alpha, duty personnel will closely monitor all unidentified personnel entering FASOTRAGRUPAC spaces and will require proper identification.

(2) Rooms and storage areas not in regular use will be secured

Encl (9)

(3) At the beginning and end of each workday and at other regular and frequent intervals, inspect for suspicious activity or packages in the interior and exterior of buildings in regular use.

b. THREATCON BRAVO. THREATCON Bravo will be implemented when an increased and more predictable threat of terrorist activity against military personnel or facilities within the San Diego area is identified. In addition to conditions set in THREATCON Alpha, the following will be implemented:

(1) Secure and regularly inspect all buildings, rooms and storage areas not in regular use.

(2) Examine all mail for letter or parcel bombs. If suspicious packages or envelopes are found in the mail, contact Security Police and evacuate the building.

(3) Things to look for when going through the mail are:

Odd-size/shaped envelopes

(b) Letters addressed to personnel not attached to the command and containing no return address.

Packages that tick or rattle

(d) Packages or envelopes with odd or unusual odors.

(e) Letters or packages with oil-like substances smeared or splattered on them.

(4) Closely monitor all personnel entering command buildings, require positive identification and spot check and inspect packages, boxes, and bags.

c. THREATCON CHARLIE. THREATCON Charlie will be implemented when an incident occurs or when intelligence is received indicating that some form of terrorist action against military personnel or facilities in the San Diego area is imminent. In addition to conditions implemented by THREATCONS Alpha and Bravo, the following will be implemented:

(1) Building access will be limited to authorized personnel only and positive identification will be required.

(2) Secure all nonessential personnel

(3) OOD, when not at meals, will remain in the duty office.

(4) Enforce centralized parking of vehicles away from sensitive buildings.

(5) Access points will be limited to one entry at each building. All other entry doors will be locked.

d. THREATCON DELTA. THREATCON Delta will be implemented when a terrorist attack has occurred against military personnel or facilities in the San Diego area or intelligence has been received that terrorist action against a specific location is likely. In addition to the conditions implemented by THREATCONS Alpha, Bravo, and Charlie, the following will be implemented:

(1) Search all suitcases, briefcases, packages, etc, brought into the command.

(2) Make frequent checks of the exterior of building and parking area.

4. ADDITIONAL ASSISTANCE. If at any time, you feel further assistance is needed, contact the NASNI Security Department.

5. THREAT ASSESSMENT. An assessment of potential threats to NAS North Island and its tenant activities is conducted yearly by the Naval Investigative Service. A copy of this assessment is kept on file by the Command Security Manager.

6. GENERAL PRECAUTIONS. The general precautions listed below should be followed in an attempt to counter terrorist attacks:

a. Be alert for strange or suspicious vehicles parked in or near command buildings. It may be a car, van, truck, or any other type of vehicle which is not normally seen in the area.

b. Be alert for individuals sitting in vehicles parked in or near command buildings, when there is no apparent reason for them to be sitting or waiting there.

c. Be alert for unidentified persons loitering around the buildings. They may be asking questions about building routine, personnel assigned to the staff, security strength, and accessibility into the buildings. This could be an indicator or pre-incident surveillance and could very well be followed by an attack or terrorist incident.

d. Be alert for persons photographing you, personnel entering and leaving buildings, or pictures of the buildings themselves. Again, it could be a sign or indicator of surveillance.

e. Be alert for unexpected visitors. This could be indicative of surveillance and also a method to gain entry. Ask for identification and then call for confirmation. Do not be afraid to deny entry to unexpected visitors.

f. Be alert for telephone inquiries which include excessive wrong numbers, surveys, or callers asking personal questions about the normal routine at the command.

g. Report any 'out of the ordinary' events to appropriate personnel, keeping the chain of command informed. If you think the event or occurrence is suspicious, report it to the NASNI Security Police, NIS, and the Executive Officer.

27 FEB 1990

HOSTAGE BILL

1. HOSTAGE SITUATIONS. A terrorist group may undertake the seizure of specific hostage(s) for ransom, media attention, coercion or political bargaining purposes. This type of crisis incident could rapidly escalate to include government agencies at the highest level.

2. Usually, the taking of hostages is connected with a terrorist attack or the taking of a specific target. Normally, by the time hostages have been taken, security force personnel, On-Scene Commander and Naval Investigative Service agents have been notified and are on the scene, directing operations or negotiating the release of hostages.

3. PROCEDURES. In the event the above is not the case, the below procedures will be followed:

- a. First and foremost, remain calm.
- b. Do not attempt rescue.
- c. Notify the NASNI OOD.
- d. Notify the FASO OOD.
- e. Notify the Executive Officer.
- f. Notify the Naval Investigative Service.

g. If possible, evacuate and secure building and wait for further instructions from NIS agents or the On-Scene Commander.

4. HOSTAGE SURVIVAL. The victim in a hostage situation can be an invaluable source of information, if he/she is somewhat prepared for what might happen. The most effective weapon the terrorist has is the hostage's fear of the unknown. Failure of potential victims to prepare for this possibility increases the effectiveness of any attempted intimidation. The ability of the hostage(s) to survive increases when he/she is aware of what is going on around him/her. The terrorist's inability to psychologically dominate his/her hostage reduces some of his/her effectiveness in dealing with the negotiator. The following guidelines are provided to aid personnel through a hostage situation:

a. Initially, one of the most important things you must do, is accept the situation and be prepared to wait.

b. Don't be a hero; there is no need. Resistance in the face of overwhelming odds can result in needless tragedy. Death or injury accomplishes nothing.

(1) Acts of violence or attempts to escape by you might provoke the the terrorist to commit an act he/she had not intended.

Encl (10)

(2) Some circumstances may be conducive to an escape attempt, but the hostage must have a clear idea of what he/she plans to do.

(3) Actions should not be simply reactions to the situation.

c. The first hour is the most dangerous. It is the most confusing time, and the terrorist is probably at his/her highest level of anxiety.

(1) Follow the instructions of your captor.

(2) The longer you are together without him/her 'getting mad' at you, the better your chances are of survival.

d. If the situation is a prolonged one, attempt to maintain control over your environment to whatever extent possible. In this way, you can view what is happening rationally. Do something to keep busy to help keep your mind off of the situation. This will counteract the terrorist's psychological pressure and enable you to keep your powers of reasoning active.

e. Do not speak to your captors unless they initiate the conversation

(1) If you get involved in a conversation, be friendly if you can, but not phony.

(2) Never offer a suggestion or plan. Let him/her do the thinking. It will keep him/her busy.

(3) If you offer a suggestion and it goes wrong, he/she may think you planned it that way.

f. Get or try to get all the rest you can during the situation. You have no way of knowing how long the situation will last, and if you are tired, you might make a mistake.

(1) Never stand when you can sit.

Sleep whenever you can.

g. If you or any of the hostages need special medication or medical help, inform your captors. Do not silently suffer. It doesn't gain anything for you.

h. Be constantly prepared for the end of the situation

Stay aware of everything you see and hear, and try to remember it.

(2) Such things as the number of captors, their descriptions, their conversations, and the types of weapons they have will be of tremendous assistance to investigators or NIS agents.

i. Most importantly, be patient. Even though the authorities may appear to be doing nothing, they are engaged in a complete program designed to rescue you unharmed as soon as possible.

j. If you believe a rescue is taking place, or hear a noise or shooting, hit the floor and stay down.

(1) Keep your hands on your head and do not make any quick moves.

(2) Remain on the floor. By remaining on the floor, even during an assault, you reduce significantly your chances of being shot.

(3) Hostages who stand up and try to run may be mistaken for a fleeing terrorist.

k. Remember, the fear of the unknown is the terrorist's most potent weapon in a hostage situation. Your ability to survive increases dramatically when you are aware of the goals the terrorists are seeking, the methods they will employ, the actions you can take to protect yourself, and the tactics which may be used to gain your release.

FIRE BILL

1. Purpose. To delineate procedures for the protection and safety of lives and property in the event of a fire.

4. Action to be taken in the event of a fire:

a. Any person who discovers a fire shall immediately activate any available fire alarm system and warn occupants to evacuate any building(s) in or near the fire. All fires, including extinguished ones, shall be reported immediately to the Fire Department. Notification can be made as follows:

(1) Exterior Fire Alarm Box. Open the door and pull down the lever. Remain at the box to direct Fire Department units to the scene of the fire.

(2) Telephone. Call the Fire Department at 9-911. State the exact location of the fire and what is burning, if known. Give your name, location and telephone number from which you are calling. DO NOT hang up until the dispatcher acknowledges all pertinent information. Proceed outside and direct arriving Fire Department units to the fire scene.

(3) Interior Alarm Box. Activate the same as an exterior fire alarm box, then proceed outside the building and direct arriving Fire Department units to the fire scene.

b. Notify the FASOTRAGRUPAC OOD (X59003) as quickly as circumstances permit.

c. If time permits, close doors and windows to confine the fire and reduce air intake. DO NOT ENDANGER YOURSELF OR OTHERS IN THIS EFFORT.

d. Use equipment on hand to extinguish the fire, pending arrival of the Fire Department. AGAIN, DO NOT ENDANGER YOURSELF OR OTHERS IN THIS EFFORT.

e. All personnel except those assigned fire fighting duties shall clear the area and those not in the immediate fire area will also evacuate to a point of safety.

3. Duties of the FASOTRAGRUPAC OOD:

a. Notify the Commanding Officer and Executive Officer.

b. Proceed to the scene of the fire and take charge until relieved by proper authority.

c. Exercise caution in utilizing personnel for the purpose of fighting fires. The low ignition potential of the buildings in the FASOTRAGRUPAC area renders firefighting therein extremely hazardous, particularly for inexperienced personnel.

Encl (11)

27 FEB 1990

d. As soon as duties permit, or when the fire is under control, muster all hands for the purpose of determining the identity of any missing persons. Submit the muster report to the Admin Department as quickly as circumstances allow.

e. Ensure all pertinent information relating to the fire is entered in the command log.

4. Duties of the FASOTRAGRUPAC Senior Watch Officer. Ensure duty section personnel are thoroughly indoctrinated in the location and use of emergency fire fighting equipment and are familiar with the contents of this fire bill.

5. Security Considerations. In the event of fire or smoke of undetermined origin, fire fighters shall be granted full access to any involved space or building. No person shall delay, deny access to, hinder, or restrict in any manner, or for any reason (security included), personnel assigned the task of saving life or property. In a fire/emergency situation, the life and safety of personnel are of paramount concern, security considerations are secondary.

6. Training. Department heads shall ensure that their personnel are properly instructed in fire prevention regulations. It is also their responsibility to provide annual training in fire prevention and first aid firefighting for their personnel. This training may be provided by Fire Department personnel upon request.

PHYSICAL SECURITY REVIEW COMMITTEE / BOARD

1. A Physical Security Review Committee (PSRC) and a Physical Security Review Board (PRSB) are established to advise and assist in applying the standards of and implementing the program for physical security and loss prevention as set forth in reference (a).

2. Physical Security Review Committee (PSRC)

a. Responsibilities. The committee will:

(1) Assist in determining requirements for and evaluating security afforded to areas of this command.

(2) Advise on establishment of restricted areas.

(3) Review draft physical security and loss prevention plan or recommended changes prior to submission to the Commanding Officer.

(4) Review reports of significant losses or breaches of security and recommended improvements to the Physical Security Prevention Program.

b. Membership. The PSRC will as a minimum include the following membership:

- (1) Security Officer (Chairperson)
- (2) Comptroller
- (3) Security Manager
- (4) ADP Security Officer
- (5) Facilities Manager
- (6) Supply Officer
- (7) Legal Officer
- (8) Code 32 Division Officer
- (9) Senior rated master-at-arms or senior designated master-at-arms
- (10) Internal Review functional manager
- (11) Building Physical Security representatives
- (12) Committee Secretary

c. Meeting and Minutes. Committee members or their representatives will meet as required, but at least quarterly. Minutes of the meeting will be made a matter of record and such records will be retained until completion of the command inspection cycle, or three years, whichever is greater.

3. Physical Security Review Board (PSRB)

a. Responsibilities. The board will coordinate naturally supportive physical security and loss prevention practices.

b. Membership. The PSRB will, as a minimum, include the following membership:

- (1) Security Officer (Chairperson)
- (2) Executive Officer (Advisor)
- (3) Comptroller
- (4) Security Manager
- (5) ADP Security Officer
- (6) Internal Review functional manager
- (7) Committee Secretary

c. Meetings and Minutes. The board will meet at least annually. Minutes of the meeting will be made a matter of record and such records will be retained until completion of the command inspection cycle, or three years, whichever is greater.

INTER/INTRA SERVICE SUPPORT AGREEMENTS (ISSA)

This command has an ISSA with the Commanding Officer, Naval Air Station, North Island (NASNI). That agreement specifically includes but is not limited to the following:

1. Law Enforcement

a. NASNI will provide investigative services and written reports regarding violations of Naval Regulations by military personnel when such violations do not fall within the Naval Investigative Service's preview.

b. NASNI will provide vehicular and pedestrian traffic control, and vehicular accident investigative services.

2. Physical Security

a. NASNI will provide routine perimeter control for the protection of FASOTRAGRUPAC resources and loss - prevention support.

b. NASNI will conduct Physical Security Review Board meetings and physical security assistance visits with written evolutions/recommendations to correct and improve any noted deficiencies.

3. Personnel Security

a. NASNI will provide a security clearance program for the access to classified material.

b. NASNI will evaluate National Agency Check (NAC) results and background investigations as required.

c. NASNI will conduct personal interviews, as required, regarding derogatory NAC results and provide written notice of actions taken.

4. Passes, Decals and Civilian Identification Badges

a. NASNI will issue civilian identification badges and provide fingerprints services, as required.

b. NASNI will issue permanent and temporary vehicle decals to this command's military and civilian personnel, as well as authorized visitors and contractors.

c. NASNI will operate a Traffic Court to adjudicate violations onboard NASNI and maintain court actions.

5. Miscellaneous. In addition NASNI will provide:

a. A Classified Material Destruction Facility

FASOTRAGRUPACINST 5530.1C

27 FEB 1990

- b. Postal and Guard Mail services
- c. Investigations of mishaps reports
- d. A Hazard Abatement Plan
- e. Federal Fire Department

SECURITY EDUCATION AND TRAINING

1. General. Every member of the Naval service and every civilian employee of the Navy and Marine Corps has a security responsibility during and after duty hours. Security awareness must be stressed by a continuous, rigorous and forceful Security Education Program. The Security Education Program is a multifaceted program which includes indoctrination training, supported by publications and briefings.

2. Requirement. A Security Education Program has been established to ensure that all assigned personnel, military and civilian, recognize, understand and carry out their responsibilities. The Security Education Program will include all pertinent aspects of physical security, law enforcement, and loss prevention programs. As a minimum this program requires:

a. Initial Security Indoctrination. All personnel military and civilian, shall receive security indoctrination training within 90 days of reporting for duty or employment. Additionally, all personnel currently assigned who have not attended a security indoctrination training course in the past shall do so within one year of the date of this instruction.

b. Reindoctrination. Security training shall be given at least annually to all military and civilian personnel after the initial indoctrination.

3. Training Objectives

a. To involve individually and collectively all military and civilian personnel in the protection of command assets.

b. To indoctrinate each individual and keep him/her proficient in the security procedures applicable to the performance of his/her duty.

c. To ensure that all personnel understand the need for security, as well as the dangers of indiscreet conversation and operational carelessness.

d. To ensure that general security measures in effect, such as the pass and badge system, privately owned vehicle inspection and control system, package inspections, etc., are fully understood by all personnel.

e. To ensure that all personnel are familiar with crime prevention programs which are designed to reduce crime, including loss of government property through pilferage.

4. Training Records and Documentation

a. Training Records. Individual security training and indoctrination records will be maintained in military service records and civilian personnel folders, as appropriate.

FASOTRAGRUPACINST 5530.1C
27 FEB 1990

b. Documentation, including curriculum outlines and copies of graphic media aids and publications will be retained until completion of the command inspection cycle or three years, whichever is longer.

MATERIAL CONTROL

1. GOVERNMENT PROPERTY. Removal of government property from this Command must be controlled to prevent loss or theft of material. Property passes are provided to permit authorized removal of government property. Personnel removing material from the Naval Air Station, North Island are subject to search per reference (j) and must have a valid property pass or other delivery document when transporting government material.

a. General. Property passes are not required for privately owned material which can be readily identified as being privately owned. Property passes are required for any articles or material which could be identified as government property. The Command AOOD and NASNI sentries will determine whether or not property passes are required.

b. Issuing Authority and Signature

(1) Signature. Property Passes (NAVSUP Form 155) can be only signed by the Executive Officer and department heads.

(2) Preparation. Persons signing property passes are responsible for ensuring that the description of the material listed on the passes agree with the contents of the package to be removed from the Command. Within the "Contents" section, all unused portions will be marked out, making additions impossible. Every property pass must show on the pass (or have securely attached to the pass) a complete list of articles to be removed from the Command. A list attached to a pass will also bear the signature of the person signing the property pass.

c. Procedures

(1) Serial Number Required. Private property passes for projectors radios, electrical appliance, or any other types of equipment which might be confused with government property, will show manufacture's name and serial number. The issuing officer will establish ownership before issued the pass.

(2) Clothing. When the owner's name on clothing coincides with the name on the member's identification card, it may be passed through without a property pass.

(3) Explosive Material. In no case will property passes be issued which will permit entrance or removal of souvenirs of an explosive character, such as ammunition, flares, etc. or any article which is dangerous to personnel engage in its handling.

d. Responsibilities

(1) Property passes will be prepared by the department concerned. One copy of a property pass is to be maintained by the Administrative Support Division (Code 12) and one copy is required at any station gate.

FASOTRAGRUPACINST 5530.1C

27 FEB 1990

(2) Naval Air Station, North Island Security Department will forward cancelled property passes to FASOTRAGRUPAC for verification. Property passes will be retained by Code 12 for a period of three months and will then be destroyed.

(3) Code 12 will maintain a log of all property passes issued and the date of their cancellation.

(4) The Administrative Officer will, on a periodic basis, furnish the Security Officer, Naval Air Station, North Island, Bldg. 605, four signature listings of those persons who are authorized to sign property passes in accordance with reference (k). Changes will be forwarded as they occur.

2. HAZARDOUS MATERIAL

a. Material normally thought to be safe may become hazardous under certain use or storage conditions. Therefore, it becomes imperative all aspects of accident prevention designed to control and regulate identification, transportation, storage, handling and use of hazardous material be implemented to protect the uses, general public and the environment.

b. Reference (1) provides the guidelines and operating procedures for the use, handling, storage and transportation of hazardous material aboard NAS North Island.

PROTECTIVE LIGHTING

1. GENERAL. Protective lighting provides a means of continuing a degree of security approaching that which is maintained during daylight hours. It increases the effectiveness of security forces performing their duties, has considerable value as a deterrent to thieves and vandals and may make the job of the saboteur or terrorist more difficult.

2. MINIMUM STANDARDS

a. Unpatrollable fence lines, water boundaries and similar areas need not be illuminated. Where these areas are patrolled, sufficient illumination shall be provided to assist the security force in preventing intrusion.

b. Vehicular and pedestrian gates used for routine ingress and egress will be sufficiently illuminated to facilitate personnel identification and access control.

c. Exterior building doors will be provided with lighting to enable the security force to observe an intruder seeking access.

d. Protective lighting will be checked daily by the security force to ensure all light fixtures are operational. Inoperative lights will be recorded and referred to the Security Officer.

e. The Security Officer will ensure that all reports of inoperative protective lights are given immediate attention and that corrective actions are taken.

f. The Security Officer will maintain a listing of all lighting system within the command.