DEPARTMENT OF THE NAVY
COMMANDER
MOBILE MINE ASSEMBLY GROUP
275 FIFTH STREET SE
CORPUS CHRISTI, TX 78419-5008

COMOMAGINST 5530.2D
N3
15 Sep 03

COMOMAG INSTRUCTION 5530.2D

Subj: PHYSICAL SECURITY PLAN

Ref: (a) OPNAVINST 5530.14C
(b) SECNAVINST 5510.36
(c) COMOMAGINST 5510.1J
(d) OPNAVINST 3300.55
(e) NASCORPCINST 5530.1A
(f) COMOMAGINST 3141.1F
(g) COMOMAGINST 3100.H
(h) OPNAVINST 5239.1B

Encl: (1) Threat Condition Procedures
(2) Bomb Threat Procedures
(3) Department of the Navy Telephonic Threat Complaint Form, OPNAV 5527/8 (12-82)
(4) Standard Form 701, Activity Security Check List

1. Purpose. This plan provides guidelines and procedures to implement physical security measures by Commander, Mobile Mine Assembly Group (COMOMAG), and defines specific actions required to safeguard personnel, prevent unauthorized access to equipment, facilities, material and documents, and protect them against espionage, sabotage, theft, or other unlawful acts. Enclosure (1) outlines procedures for threat conditions. Enclosure (2) outlines procedures to follow in the event of a bomb threat. Use enclosure (3) to record pertinent information regarding a bomb threat. This is a major revision to the basic instruction and should be reviewed in its entirety.

2. Cancellation. COMOMAGINST 5530.2C.

3. Responsibilities

a. The Commander (CDR) is responsible for ensuring appropriate measures are taken to safeguard personnel and property within the facility, 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 command.

b. Physical Security Officer (PSO). The PSO is responsible for planning, coordinating, and supervising the COMOMAG physical security program. The PSO is also responsible for:

(1) All matters pertaining to physical security.

(2) Formulating emergency plans and activating the plans when directed by or on behalf of the CDR.

(3) Reviewing and updating the COMOMAG physical security plan as required.

(4) Complying with other related duties as specified in paragraph 0111 of reference (a).

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

c. Physical Security Review Committee (PSRC). The Physical Security Review Committee will consist of the Chief Staff Officer (CSO), all department heads, Physical Security Officer (PSO), Automated Information Systems Security Officer (AISSO) and the command facilities representative. Per reference (a), the committee will:

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

(2) Advise on establishing restricted areas.

(3) Review the physical security plan, loss prevention plan and any recommended changes prior to submission to the CDR.

(4) Review reports of significant losses or breaches of security and, based on analysis of such instances, recommend improvements.

(5) Meet at least quarterly and make a written report to the CDR.

c. Loss Prevention Subcommittee. Due to the small size of the command, the PSRC will perform the duties of the LPS per reference (a).

d. Physical Security Review Board (PSRB). The PSO will attend the PSRB meetings aboard Naval Air Station Corpus Christi. Minutes of the meeting will be provided to the Physical Security Review Committee during the next scheduled meeting.

e. Military Personnel and Civilian Employees. All personnel will be responsible for adhering to security practices set forth in this plan and become familiar with evacuation procedures during emergency situations.

f. Control of Information. Effective control of classified and sensitive information will be maintained at all times per references (b) and (d) . Effective control requires that dissemination be limited, excessive reproduction prevented, and a minimum level of classified documents maintained.

g. Classified Material Transport between buildings 36, 37 and 39. Per reference (b), classified material will be transferred from building 36; building 37 and building 39 as follows:

(1) Classified material will be placed in an envelope and properly marked with the correct classification of the highest marking.

(2) A brief case may be used as the outer wrapper or the package will be sealed in another envelope. Courier cards are required by individuals who are transporting classified material from one building to another.

(3) Emergency Planning. Should an emergency arise requiring protection or destruction of classified documents, procedures in Appendix A Emergency Action Plan for Protection of Classified Material.

h. Storage. All classified documents will be stored in an authorized container per references (b) and (c) when not in use.

i. Destruction. Destruction of classified material shall be accomplished per references (b) and (c), and under the cognizance of the CSM.

4. Personnel Access Identification and Movement

a. Definitions

(1) Employee. Any military or civilian who is paid from federally appropriated or Non-appropriated funds and assigned to work at COMOMAG.

(2) Contract Employee. An individual working for a contractor and whose work site is this command.

(3) Visitor. Any person, civilian or military, who is not permanently employed by COMOMAG or permanently, assigned to work in COMOMAG spaces.

(a) Official Visitor. Any person, civilian or military who is conducting a legitimate service or business at COMOMAG.

(b) Unofficial Visitor. All other personnel not visiting COMOMAG in an official capacity, i.e. family members, personal visits, etc.

(4) Escort System. Escorting is a method to control all non official visitors, and any other visitors without the appropriate security clearance for the restricted area visited. Escort personnel may be civilian or military personnel and will normally be from the office of the person visited.

(5) Restricted Area. As established in writing by the CDR within his/her jurisdiction.

b. Access Control

(1) Access control at COMOMAG headquarters building is achieved by a personnel identification system (security badges), swipe cards, the escort system, and controlled ingress/egress points.

(2) All personnel who require access for reasons of employment or official business, individuals who render a service, dependents; retired military and unofficial visitors will be positively identified prior to entry.

(3) All personnel within COMOMAG headquarters building, shall display or be accompanied by a person displaying a Mobile Mine Assembly Group or Commander, Mine Warfare Command security badge It is the responsibility of all hands to be constantly Vigilant and to ensure that personnel within COMOMAG headquarters building comply with this requirement.

(4) A security clearance is not required for unescorted access to COMOMAG. However, the appropriate level security clearance and the need-to-know is required for access to classified information. All hands are responsible for the protection of classified material.

c. Area Designation. The complete interior of COMOMAG Headquarters building 36 is designated a level ONE restricted area.

d. Security Badges

(1) Security badges indicating a security clearance will not be issued without prior verification of identification (state, or government ID with photograph) and clearance level from a command approved source.

(2) All COMOMAG employees shall be issued a permanent COMOMAG

security badge with a recognizable photograph of the bearer, and security clearance color code sealed within the laminate.

(3) Visitors that do not possess an approved security badge and require unescorted access or access to classified information will complete the information required in the visitors log on the quarterdeck and receive issue of a temporary (non-picture) badge indicating the verified level of clearance.

(4) COMOMAG and COMINEWARCOM security badges are identical in appearance with the exception of the command name across the bottom of the badge. COMINEWARCOM and COMOMAG permanent badges utilize the color of the printed lettering to identify the clearance level. CMWC temporary badges are disposable color coded paper with a clearly visible expiration date written on the badge at the time of issue. Clearance color codes are as follows:

(a) Yellow Badges. Issued to all visitors who do not have a current security clearance on file. Should be escorted by an employee of the department being visited.

(b) Blue Badges. Issued to all visitors that have a current Confidential clearance on file. This badge authorizes personnel to move around the building unescorted. This badge does not give the person authority to enter any restricted area.

Those staff members who are responsible for the restricted area must grant permission for individuals to enter their area with an appropriate escort.

(c) Red Badges. Issued to all visitors that have a current Secret clearance on file. This badge authorizes personnel to move around the building unescorted. This badge does not give the person authority to enter any restricted area. Those staff members who are responsible for the restricted area must grant permission to individuals not on the access list to enter their area.

(d) Orange Badges. Issued to all visitors that have a current Top Secret clearance on file. This badge authorizes personnel to move around the building unescorted. This badge does not give the person authority to enter any restricted area. Those staff members who are responsible for the restricted area must grant permission to individuals not on the access list to enter there are.

(e) White Badges. Issued to all visitors that have a current Top Secret/SCI clearance on file. This badge authorizes personnel to move around the building unescorted. This badge does not give the person authority to enter any restricted area. Those staff

members who are responsible for the restricted area must grant permission to individuals not on the access list to enter their area. Note: red, orange and white badges are controlled items and are in custody of the Physical Security Manager.

(f) The Physical Security Officer will issue all permanent badges for COMOMAG staff members. COMOMAG staff members who do no have their badges must sign in at the quarterdeck and be issued a visitor's list.

Note: Due to staffing shortage, janitors and Public Works employees will be able to walk around without an escort. As a caution to all staff, you must sanitize your area when they are in the area.

5. Intrusion Detection System (IDS). The IDS is designed to detect, not prevent actual or attempted penetrations. The IDS at COMOMAG consists of essentially two separate systems (zones), the general building and N5 spaces. When either zone is in a alarm condition the same electronic signal leaves the command. The system is a monitored by the CMWC Quarterdeck and the host command monitoring station.

a. Responsibility

(1) The SO shall be responsible to ensure a reliable IDS is maintained and personnel are adequately trained for operation and response to various alarm conditions.

(2) N5 personnel shall activate the N5 space IDS for operation during non-working hours.

(3) Duty personnel shall activate the building IDS at the conclusion of security checks for operation during unoccupied hours. COMINEWARCOM N6 and N2A personnel are also authorized to activate building IDS if COMOMAG duty personnel have departed for the day. Note: COMINEWARCOM N6 and N2A personnel shall notify the SDO upon enabling or disabling the IDS.

b. Maintenance. Will be performed in accordance with required routine schedules. Emergency service will be performed <u>immediately</u>. A service contract is in place for the maintenance of the system. Random tests of system sensors will be performed monthly and records kept of test results. All maintenance will be logged. When the system is being repaired, the maintenance person will have an escort at all times.

c. Alarm Response. The most likely time of an alarm is when the building or N5 spaces are unoccupied because the IDS is not activated until all personnel have departed. Upon alarm activation CMWC will contact the COMOMAG SDO for appropriate action.

(1) IF THE CAUSE OF ALARM IS SUSPECT, WAIT FOR BASE POLICE TO ENTER AND SANITIZE THE BUILDING.

(2) If the known cause of alarm was inadvertent, call base police immediately and advise of the situation. Base police may still arrive for a security check.

d. AC Power failure. The IDS is equipped with a four hour backup power supply when normal AC power is lost or interrupted.

6. Key and Lock Control. The PSO shall manage and supervise the command key and lock control program. Due to the physical size of COMOMAG the SO will also assume the duties of the Key Control Officer as outlined in reference (a). Keys are maintained in a locked key cabinet located in radio and the quarterdeck. Keys are issued to staff personnel only. A Key Control Custodian shall be designated in writing who is responsible to the PSO for the control, inventory and records of program assets.

a. Key Control. All keys utilized for the protection of restricted areas, critical assets, classified material/equipment, sensitive material and supplies shall be controlled and accounted for on a key control register. Continuous accountability/ issuance of controlled keys shall be recorded in a key control log with the following information provided:

(1) Key serial number

(2) Printed name and signature of person taking custody

(3) Date/time of issuance and return

b. Criteria for Issuing Keys. Controlled keys will be permanently issued only to those persons with a need and as approved by the CDR, CSO, or PSO. Temporary issue will only be to COMOMAG employees on a as needed basis, not to exceed the end of normal working hours, unless approved by appropriate authority. The SO is responsible for enforcing key issuance and approval of all requests for additional keys or deletions of keys in the program.

c. Lost or Damaged Keys and Locks. In the event of lost, misplaced, or stolen keys, the affected locks or cores to locks, shall be replaced immediately. Replacement or reserve locks, cores, and keys will be secured to preclude accessibility by unauthorized individuals. The PSO will be notified immediately in the event or damaged or missing controlled keys or locks.

d. Inventories of Controlled Keys. The Key Control Custodian shall inventory all controlled keys at least quarterly and provide

inventory results to the PSO. The PSO will audit the Controlled Key and Lock Program annually. All inventories and audits will be recorded and retained for three years or completion of the next command inspection whichever is greater.

7. Loss Prevention Plan. The COMOMAG Loss Prevention Plan is designed to reduce the loss of government property. These losses are incurred through theft, vandalism, and misappropriation. This plan is designed to identify the causes of losses, establish procedures to analyze the cause and recommend preventive measures to preclude future losses. This plan applies to all personnel assigned to COMOMAG.

a. Accountability. Property accountability entails inventory and inspection procedures. The loss prevention plan requires COMOMAG to conduct an annual inventory of assigned equipment.

b. Susceptibility. Property most susceptible to theft is likely to have a high value and/or civilian use. Electronic items such as typewriters, computers, calculators, printers and recorders are particularly attractive and susceptible to theft.
All COMOMAG personnel must ensure all highly susceptible property is properly documented and inventoried.

c. Material Control. Government property will be kept within COMOMAG spaces. Government property will only be removed when authorized by the appropriate Department Head. The bearer will have a property pass authorizing removal and possession of said property. Property passes will be in duplicate, the original to be held by the authorized person, and the duplicate to be retained on file. The original will be returned to the Department Head when the material is returned. The department property pass book will be held by the Department Head and will be available to Supply during inventories to account for missing property.

d. Missing Lost Stolen Report Procedure. Missing, lost, or stolen government property will be reported per reference (b), and accountable individuals will be identified. Property inventories will be matched with existing property.
Investigations will be submitted with loss reports. The SO is the focal point for tracking such reports.

e. Reporting of Losses. Reporting losses of government property should be made immediately to the Security Officer by the individual making the discovery. The SO will contact the Naval Air Station Corpus Christi Security Department, local Naval Criminal Investigative Service (NCIS) Agent, and Commander, Mine Warfare Command as necessary. They will be the primary resources for detection and

investigation of lost, stolen or missing government property. All government property lost or missing, regardless of value or classification will be reported to the SO for investigation. Appropriate documentation regarding missing, lost, stolen or recovered government property will be accomplished per reference (b).

f. Personnel Education. The PSO will establish a program of indoctrination in the COMOMAG Security Program for all newly reporting military and civilian personnel. All personnel will be indoctrinated in their responsibility for the care and protection of government property under their control/custody and the administrative and criminal consequences of involvement in its loss/theft. Personnel currently assigned are required to attend a security briefing at least quarterly.

g. Administrative Inspections. All hand carried items, such as brief cases, bags, boxes, etc., are subject to inspection prior to entering and before departing COMOMAG office spaces. The inspections will be accomplished as directed by the CO.

8. Internal Classified Document Control Procedures

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

b. Control of Information. Effective control of classified and sensitive information will be maintained at all times per reference (c). Effective control requires that dissemination be limited, excessive reproduction prevented, and a minimum level of classified documents maintained. Individuals who become aware of the loss, compromise or possible compromise of classified information or material are to immediately notify their Security Manager or Commanding Officer.

c. Storage. All classified documents, when not in use, will be stored in an authorized container per references (c) and (d).

d. Destruction. Destruction of classified material shall be accomplished per references (c) and (d), and under the cognizance of the CSM.

e. Emergency Planning. Should an emergency arise requiring protection or destruction of classified documents, procedures in reference (c) will be carried out.

9. Security Checks. End of the day security checks shall be performed prior to securing any space within a restricted area with particular attention to the secure storage of classified material,

fire hazards, windows and doors locked where appropriate. The use of Standard Forms 701, 702 are mandatory and retained for the record as determined by the CSM. When used properly, these forms prevent common security and safety discrepancies.

a. Responsibilities

(1) Cognizant personnel shall perform security checks and complete SF 701 and 702. Areas not accessible to the watch during security checks shall maintain the SF 701 outside the door.

(2) Duty personnel shall conduct a security check of building 36 prior to securing for the day to include:

(a) A physical check of all accessible security containers, annotating SF 702 as locked and checked.

(b) Review posted SF 701's for proper closure of areas not accessible.

(c) Head and passageway windows/doors secure.

(3) Cognizant departments shall ensure areas not normally used for daily business will remain locked if practical, and will be unlocked by appropriate staff personnel when access is required.

(4) Significant problems should be noted and reported to cognizant department head immediately.

b. Protective Lighting. Command security lighting shall be illuminated during the hours of darkness.

Non illuminated security lighting shall be expeditiously reported to the SDO for appropriate action. Necessary work request shall be submitted not later than the next business day.

10. Communications. COMOMAG spaces have several telephones in each office. Each of these phones have several incoming/outgoing nonsecure voice lines. Classified information will not be discussed over these telephones. Classified conversations will only be held on the STU-III phones provided in the offices that require them. Telephonic Threat Complaint forms, enclosure (2), are located adjacent to all phones in the event a threat is made via telephone.

11. Destructive Weather. COMOMAG will follow the procedures in reference (f) when destructive weather threatens COMOMAG and the Corpus Christi area.

12. Fire Plan. In event of fire, personnel will respond and follow the guidelines delineated in COMOMAGINST 3100.1H, Command Fire Bill, reference (g).

13. Emergency Action Plans. COMOMAG will comply with the Naval Air Station Physical Security Instruction, reference (e), as applicable.

14. Automated Information System Security Officer (ISSO). The IISO will ensure the Automated Data Processing equipment is operated per reference (h).

T. W. AUBERRY

Distribution: (COMOMAGINST 5216.1T)
List I
List II, Case A
List II, Case B (COMINEWARCOM only)
NAS, Corpus Christi, TX (Security Dept)

THREAT CONDITIONS

1. Terrorist Threat Conditions (THREATCONS) and Measures. Information and Warnings of terrorist activity against **COMOMAG** and NAS Corpus Christi will normally be received from security authorities or through security agencies. Information may come from local police, be received directly by the command as a threat or warning from a terrorist organization, or be in the form of an attack.

2. Purpose. To inform COMOMAG personnel of terrorist THREATCONS for the command.

3. Declaration of Terrorist **THREATCONS** and Measure Implementation. The declaration of THREATCONS and implementation of measures may be decreed by COMOMAG following receipt of intelligence through official sources or an anonymous threat message. Lateral and vertical reporting will occur to ensure notice of the THREATCON is given to other potentially affected areas. The following guidelines are provided.

a. Threat Assessment Guidelines. The following general guidelines are provided for uniform implementation of security alert conditions. Assessment factors are defined as follow:

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

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

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

(a) History. Demonstrated terrorist activity over time.

(b) Targeting. Current credible information on activities indicative of preparations for specific terrorist operation.

(c) 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 a combination 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, and history must be present.

(3) Medium. Factors of existence, capability, and history 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.

C. Environment. Security environment is considered separate as a modifying factor and may influence the assigned threat level. These limitation guidelines apply only to the assessment of a terrorist threat against U.S. or DOD interest.

4. Threat Analysis. Ideally, an intelligence estimate/threat analysis would be a routine, continuous function preformed by the NCIS, NAS Corpus Christi, in support of the command. U.S. government agencies acting as excellent sources of information include the Federal Bureau of Investigation which is responsible for dealing with terrorism involving U.S. military personnel on naval stations everywhere. The Naval Investigative Service will provide liaison between U.S. Navy assets and other government agencies.

5. Threat Conditions.

a. **THREATCON ALPHA**. A general warning of possible terrorist activity, the nature and extent of which are unpredictable, where circumstances do not justify full implementation of the measures contained in THREATCON BRAVO. However, it may be necessary to in this threat condition must be capable of being maintained indefinitely.

(1) Measure 1. At regular intervals, remind all personnel, including dependents, to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Be alert for unidentified vehicles on or in the vicinity of naval installations, abandoned parcels, suitcases, or any unusual activity.

(2) Measure 2. Keep available at all times appointed personnel who have access to plans for evacuating buildings and areas in use and for sealing off areas where an explosion or attack has occurred. Keep key personnel on call who may be needed to implement security plans.

(3) Measure 3. Secure rooms and storage areas not in regular use.

(4) Measure 4. Do security spot checks of vehicles and persons entering the building.

(5) Measure 5. Regularly inspect all rooms and storage areas not in regular use.

b. **THREATCON BRAVO**. This condition is declared when there is increased and more predictable threat of terrorist activity even though no particular target has been 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.

(1) Measure 6. Repeat Measure 1 and warn personnel of any other form of attack to be used by terrorist.

(2) Measure 7. Keep all personnel involved in implementing anti-terrorist contingency plans on call.

(3) Measure 8. Check plans for implementation of the measure contained in the next THREATCON.

(4) Measure 9. When possible, cars and objects such as crates, trash containers, etc., are to be moved at least 80 feet (25 meters) from the building.

(5) Measure 10. Secure and regularly inspect all rooms and storage areas not in regular use.

(6) Measure 11. At the beginning and end of each workday and at regular and frequent intervals, inspect for suspicious activity or packages, and the interior and exterior of buildings in regular use.

(7) Measure 12. Examine all mail for letter or parcel bombs. (This examination is increased above normal).

(8) Measure 13. Make staff and dependents aware of the general situation to stop rumors and prevent unnecessary alarm.

(9) Measure 14. Upon entry of visitors to the command, physically inspect their suitcases, parcels, and other containers.

c. **THREATCON CHARLIE.** This condition is declared when an incident occurs or when intelligence is received indicating some form of terrorist action against the command or personnel is imminent. Implementation of this measure for more than periods will probably create hardship and will affect the peacetime activities of the command and its personnel.

(1) Measure 15. Continue all **THREATCON BRAVO** measures or introduce those outstanding.

(2) Measure 16. Keep all personnel who are responsible for implementing anti-terrorist plans available at their places of duty.

(3) Measure 17. Limit access points to absolute minimum.

d. **THEATCON DELTA.** A terrorist attack has occurred or intelligence has been received that terrorist action against the command is likely. Normally, this **THREATCON** is declared as a localized warning.

(1) Measure 18. Continue or introduce all measures listed for THREATCON BRAVO AND CHARLIE.

(2) Measure 19. Control all access points and implement positive identification of all personnel.

(3) Measure 20. Make frequent checks of the exterior of the building and parking area.

(4) Measure 21. Minimize all administrative journeys and visits.

e. Specific guidelines for all **THREATCONS** are outlined on pages 2-9 to 2-13 of reference (a).

BOMB THREAT PROCEDURES

1. Procedures for Handling Bomb Threats/Bombs

a. If possible, summons assistance from any nearby staff members to call the operator and attempt to trace the call, have the phone number ready that the threat is received on. Additionally, calls to the police, SDO and chain of command can be initiated.

b. Obtain the maximum amount of information from the source as possible. Attempt to record every word, utilizing the telephonic complaint form (enclosure (2). Explain to the caller that you would like them to answer a few questions to determine if this is a real bomb threat.

c. Ask the questions:

(1) When is the bomb going to explode?

(2) Where is the bomb?

(3) What kind of bomb is it?

(4) What does the bomb look like?

(5) Who are you and where are you calling from?

d. Listen closely to the voice of the caller and for any background noise and attempt to determine the following information:

(1) Sex of Caller.

(2) Age of Caller.

(3) Accent (Is the voice native to the area?)

(4) Speech impediments or peculiar voice characteristics.

(5) Attitude of Caller - Calm? Excited?

(6) Record a description of any and all background noise.

DO NOT HANG UP THE PHONE LINE, KEEP THE LINE OPEN EVEN AFTER THE CALLER HANGS UP.

e. Immediately notify the SDO, chain of command, CMWC, base police, NCIS and Senior Officer Present Ashore (SOPA), if not already accomplished.

f. The SDO or senior person present will assume the authority of on-scene commander until relieved by proper authority, and direct all personnel to carry out instructions.

g. Evacuating the building using the command telephone intercom system making the following statement:

ATTENTION IN THE BUILDING - ATTENTION IN THE BUILDING, THIS IS (identify yourself), COMOMAG HAS JUST RECEIVED A PHONE CALL THAT REQUIRES BUILDING EVACUATION.

ALL PERSONNEL SHALL SECURE CLASSIFIED MATERIAL AND EXIT THE BUILDING WITHOUT DELAY. REPORT ANY NEW, UNUSUAL PACKAGES OR CONTAINERS THAT MAY BE NOTICED DURING YOUR DEPARTURE TO THE ON SCENE COMMANDER ONCE YOU ARE IN THE ASSEMBLY AREA.

PROCEED NOW TO THE ASSEMBLY AREA LOCATED AT CENTER FIELD, TOWARDS CNATRA.

h. ON-scene commander shall ensure the following is accomplished:

(1) Send road guards to maintain a safety zone of 300 feet from passing vehicular and pedestrian traffic other than emergency responders.

(2) Names and any statements of evacuees are recorded.

(3) Make notifications not already accomplished, initiate Unit SITREP for threats that are false or a hoax. Initiate OPREP-3 NAVY BLUE when a Improvised Explosive Device is found or has exploded.

i. The senior law enforcement representative and the on scene Commander shall determine the method of search based on resources and the threat's credibility. Options include:

(1) Threat credibility considered **VERY LOW**. Command designated individuals search assigned areas. **If any suspect objects are found, do not handle or disturb, make reports to Explosive Ordnance Disposal (EOD).**

(2) Threat credibility considered **LOW.** Occupants search their own areas due to familiarity and the ability to complete the search quickly. **If any suspect objects are found, do not handle or disturb, make reports to EOD.**

(3) Threat credibility considered **HIGH**. Trained law enforcement personnel and or explosive sniffing dogs conduct a very thorough search.

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?**

1. 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

a. 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 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

9. 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 Co. ☐ EOD ☐ Fire Dept.

CLEAR

ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

TO *(If required)*	FROM *(If required)*	THROUGH *(If required)*

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Windows and doors have been locked (where appropriate).																															
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.																															
5. Security alarm(s) and equipment have been activated (where appropriate).																															
INITIAL FOR DAILY REPORT																															
TIME																															