COMNAVRESFOR INSTRUCTION 5500.3A CHANGE TRANSMITTAL 2

Subj: COMMANDER, NAVAL RESERVE FORCE (COMNAVRESFOR) SECURITY MANUAL

Encl: (1) Revised page iii
      (2) New Chapter XIX, pages XIX-1 through XIX-3

1. Purpose. To issue change 2 to the basic instruction.

2. Action

   Remove page iii of the basic instruction and replace with enclosure (1) of this change transmittal.

   c. Add enclosure (2) of this change transmittal after chapter XVIII.

Distribution: (COMNAVRESFORINST 5218.2)
List A (A3 (CNO (N095)) only)
   B1
   B2 (less FT10, 26Z1, RPAAT PAC/LANT, NAMTRAGRU COMNAVAIRESFOR LIAISON, and FT24)
   C1 (26R1, 26R2 only)
   C2 (FR7 only)
   D
   E2 (26W1, 26W2, and 26TTT only)
COMNAVRESFOR INSTRUCTION 5500.3A CHANGE TRANSMITTAL 1

Subj: COMMANDER, NAVAL RESERVE FORCE (COMNAVRESFOR) SECURITY MANUAL

Encl: (1) Revised pages 1 through 3
     (2) Revised page iii
     (3) Revised Chapter XVI, pages XVI-1 and XVI-2
     (4) New Chapter XVIII, pages XVIII-1 through XVIII-8

1. Purpose. To issue change 1 to the basic instruction.

2. Action
   a. Remove pages 1 through 3 of the basic instruction and replace with enclosure (1) of this change transmittal.
   b. Remove pages iii and iv of the basic instruction and replace with enclosure (2) of this change transmittal.
   c. Page I-2, subparagraph 3b(1) (h), delete ". Ensure semiannual sweeps are conducted which will include one drill weekend”.
   d. Remove chapter XVI of the basic instruction and replace with enclosure (3) of this change transmittal.
   e. Add enclosure (4) of this change transmittal after chapter XVII.

Distribution: (COMNAVRESFORINST 5216.1J)
List A (A3 (CNO (N095)) only)
   B1
   B2 (less RPAAT, NAMTRAGRU COMNAVAIRESFOR LIAISON, 21A3, and FT24)
   C1 (26R1, 26R2 only)
   C2 (39R only)
   D
   E2 (26W1A, 26ITT only)

ROBERT F. SANDWEG
Chief of Staff
Subj: COMMANDER, NAVAL RESERVE FORCE (COMNAVRESFOR) SECURITY MANUAL

Ref: (a) NWP1-01 (The Naval Warfare Publication System)
(b) OPNAVINST 5510.1H (Department of the Navy Information and Personnel Security Program Regulation)
(c) OPNAVINST 5530.14B (Department of the Navy Physical Security and Loss Prevention Manual)
(d) OPNAVINST 5530.15 (Physical Security Joint Services Pub)
(e) SECNAVINST 5530.4B (Naval Security Forces Ashore and Afloat)
(f) OPNAVINST 5580.1 (Navy Law Enforcement Manual)
(g) NAVOP 028/92 (Weapons and Violence)
(h) OPNAVINST 11010.20E (Facilities Projects Manual)
(i) SECNAVINST 5511.36A (Authority of Military Commanders under the Internal Security Act of 1950 to Issue Security Orders and Regulations for the Protection of Property and Places under their Command)
(j) COMNAVAFRESFORINST 5720.11A (Commander, Naval Air Reserve Force Sponsored Air Show/Open House Events, Policy Guidance)
(k) OPNAVINST 5605.19J (U.S. Navy Distribution Procedures for COMTAC and Joint Doctrine Publications)
(l) SECNAVINST 5500.29B (Use of Force by Personnel Engaged in Law Enforcement and Security Duties)
(m) OPNAVINST 1020.4C (Standard for Wearing Camouflage Utility Uniform by Navy Security Force Personnel)
(n) OPNAVINST 5530.13B (Department of the Navy Physical Security Instruction for Sensitive Conventional Arms, Ammunition and Explosives (AA&E))
(o) NAVSEAINST 8370.2 (Small Arms and Weapons Management Policy and Guidance Manual)
(p) SECNAVINST 5500.4G (Reporting of Missing, Lost, Stolen, or Recovered Government Property)
(q) SECNAVINST 5500.31A (Technical Surveillance Countermeasures (TSCM) Program)
(r) OPNAVINST C5510.101D (NATO Security Procedures (NOTAL))
(s) NAVOP 3300.53 (Navy Combating Terrorism Program)

1. Purpose. To consolidate existing Department of the Navy and COMNAVRESFOR instructions on security and related regulations/publications into one document for the management and coordination of Reserve-wide Navy security programs and to implement the Navy’s security programs within COMNAVRESFOR’s claimancy. This includes policy, guidance, and assignment of responsibilities for the security of personnel, property, information, and material assigned to the Naval Reserve. This instruction has major revisions incorporated and should be read in its entirety.

2. Cancellation. COMNAVRESFORINST 5500.3, COMNAVRESFORINST 5510.6, and COMNAVRESFORINST 5820.1.

3. Scope. COMNAVRESFOR’s emphasis on security extends to all Naval Reserve commands, and applies equally to all active and inactive duty military, and civilian personnel assigned to or associated through employment with the COMNAVRESFOR claimancy.
4. **Action.** All echelons of command shall establish security programs commensurate with their needs, using references (a) through (s) and this instruction for guidance.

5. **Forms**

   a. The following forms are available through normal Navy supply channels per NAVSUP P2002D using the National Stock Numbers (NSNs) cited:

      - **OPNAV 5512/2**  
        Authorization to Carry Firearm  
        NSN 0107-LF-055-1400

      - **OPNAV 5560/1**  
        Non-Government Vehicle Registration  
        NSN 0701-LF-055-6005

      - **OPNAV 5510/413**  
        Personnel Security Action Request  
        NSN 0107-LF-009-4200

      - **NAVRES 5532/1**  
        Visitor and Vehicle Registration Log  
        NSN 0117-LF-055-3205

      - **OPNAV 5511/13**  
        Record of Disclosure  
        NSN 0107-LF-055-1165

      - **OPNAV 5527/8**  
        Telephonic Threat Complaint  
        NSN 0107-LF-055-2740

      - **OPNAV 5511/10**  
        Record of Receipt  
        NSN 0107-LF-008-8000

      - **OPNAV 5070/11**  
        Library Catalog Card  
        NSN 0107-LF-050-7055

      - **OPNAV 5070/12**  
        Change Entry Certification Form  
        NSN 0107-LF-050-7062

   b. **CNET-GEN 5512/3 and 5512/8** may be obtained by submitting, through your supply system, a DD-1348 to Commanding Officer, Navy Supply Center (Code 101.3), Naval Air Station, Pensacola, FL 32508-6200:

      - **CNET-GEN 5512/3**  
        Pass Application  
        NSN 0197-LL-NF3-1341

      - **CNET-GEN 5512/8**  
        Temporary Vehicle Pass  
        NSN 0197-LL-NF3-1391

   c. **Optional Form 55** may be obtained from the General Services Administration:

      - **OPTIONAL FORM 55**  
        U.S. Government Identification  
        NSN 7540-00-926-8842

   d. The following forms may be obtained by submitting a memorandum to COMNAVRESFOR (N01A2), 4400 Dauphine St., New Orleans, LA 70146-5046:

      - **NAVRES 5580/1**  
        Deadly Force Certification

      - **DAAG Form 29**  
        Subregistry/Control Point Signature List

   e. The **NAVRES 5511/5** (Classified Material Control Form) is a computer generated form.
6. Reports

   a. The NATO Annual Inspection/Inventory requirement contained in paragraph 5 of chapter 15 of this instruction has been assigned report symbol COMNAVRESFOR 5510-2. This requirement will remain in effect for 6 years from the date of this directive.

   b. The requirement to report incidents of possible compromise or actual compromise contained in paragraph 4a(6) (e) of chapter 15 of this instruction has been assigned report symbol OPNAV 5510-6B per reference (b).

Distribution: (COMNAVRESFORINST 5216.1J)
List A (A3 (N095) only)
   B (less RPAAT PAC/LANT, NAMTRAGRU COMNAVARESFOR LIAISON, FT24)
   C1 (26R1, 26R2, only)
   C2 (39R only)
   D
   E2 (26WIA, 26TTT only)

Stocked:
COMNAVRESFOR (N01A)
# Table of Contents

**Letter of Issuance**

**Cross Reference (Locator) sheet** (unnumbered)

**Record of Changes**

**Table of Contents**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Program Management</td>
<td>I-1</td>
</tr>
<tr>
<td>II. Base/Shore Facilities Physical Security</td>
<td>II-1</td>
</tr>
<tr>
<td>III. Shore Activities Physical Security Plans</td>
<td>III-1</td>
</tr>
<tr>
<td>IV. Security Forces</td>
<td>IV-1</td>
</tr>
<tr>
<td>V. Auxiliary Security Forces (ASF)</td>
<td>V-1</td>
</tr>
<tr>
<td>VI. Security Education</td>
<td>VI-1</td>
</tr>
<tr>
<td>VII. Security of Sensitive Conventional Arms, Ammunition and Explosives</td>
<td>VII-1</td>
</tr>
<tr>
<td>VIII. Threat/Security Conditions</td>
<td>VIII-1</td>
</tr>
<tr>
<td>IX. Information and Personnel Security</td>
<td>IX-1</td>
</tr>
<tr>
<td>X. Loss Prevention</td>
<td>X-1</td>
</tr>
<tr>
<td>XI. Law Enforcement/Security Office Forms</td>
<td>XI-1</td>
</tr>
<tr>
<td>XII. Bomb Threats</td>
<td>XII-1</td>
</tr>
<tr>
<td>XIII. Flightline Physical Security</td>
<td>XIII-1</td>
</tr>
<tr>
<td>XIV. Crime Prevention</td>
<td>XIV-1</td>
</tr>
<tr>
<td>XV. Safeguarding North Atlantic Treaty Organization (NATO) Classified Materials</td>
<td>XV-1</td>
</tr>
<tr>
<td>XVI. Industrial Security</td>
<td>XVI-1</td>
</tr>
<tr>
<td>XVII. Combating Terrorism</td>
<td>XVII-1</td>
</tr>
<tr>
<td>XVIII. Naval Warfare Publications (NWP)</td>
<td>XVIII-1</td>
</tr>
</tbody>
</table>

**APPENDIX A**

Course of Instruction - Auxiliary Security Force (ASF)  
A-1

**APPENDIX B**

Bomb Threats  
B-1

**APPENDIX C**

Part 1-Flightline Physical Security  
C-1
Part 2-Minimum Flightline Physical Security Standards  
C-2
Part 3-Tenant Activity Support Responsibilities  
C-4
Part 4-Flightline Personnel Control Procedures  
C-5
Part 5-Flightline/Support Facility Badges  
C-6
Part 6-Flightline Vehicle Control Procedures  
C-10

**APPENDIX D**

Accountability and Control of Classified Material  
D-1

**APPENDIX E**

Part 1-NATO Classified Material Briefing Guide  
E-1
Part 2-NATO Inspection Checklist  
E-5

**APPENDIX F**

Lesson Topic Guide  
F-1
CHAPTER XVI
INDUSTRIAL SECURITY

1. Background. On 30 September 1994 the National Industrial Security Program Operating Manual (NISPOM) was signed by the Secretary of Defense. The NISPOM represents a coordinated effort to streamline policy and eliminate nonvalue added security requirements from the industrial security program. Change 5 to reference (b) implements the NISP within the Department of the Navy and expands the industrial security responsibilities of commanding officers.

2. Policy. Commanding officers must establish an industrial security program if cleared contractors are operating within areas under their direct control.

3. Responsibilities

a. COMNAVRESFOR (N01A2) is responsible for the COMNAVRESFOR Industrial Security program and will:
   (1) Provide policy, direction, and guidance to field activities on implementation of the industrial security program,
   (2) ensure, through oversight inspections, that field activities are conducting their industrial security program per the requirements of reference (b) and this instruction, and
   (3) provide technical expertise to field activities on matters relating to the industrial security program.

b. Commanders/commanding officers will:
   (1) Establish security oversight for classified contractor work, and
   (2) provide appropriate guidance consistent with reference (b) whenever cleared contractor operations are present.

c. Command security managers shall:
   (1) Serve as the commanding officer’s advisor and direct representative in matters pertaining to industrial security,
   (2) ensure compliance with the requirements of reference (b) when access to classified information is provided contractor personnel, and
   (3) ensure contract personnel are integrated into the command security education and awareness program.

4. Contractor Operations. When contractor employees are involved in work that requires access to classified material, commands must take specific measures to establish oversight for the classified work. Within the Naval Reserve the following measures will be taken as a minimum:
   a. Review the contract provisions as they relate to handling and safeguarding of classified material. Request a copy of the Contract Security Classification Specification (DD Form 254) from the contracting officer and ensure it adequately addresses security requirements.
   b. Ensure, prior to releasing classified material, contractor personnel are properly cleared and the command has on file a visit request with the following information:

XVI-1
(1) Contractor’s name, address, and telephone number, assigned CAGE Code, if applicable, and certification of the level of the facility security clearance;

(2) name, date and place of birth, and citizenship of the employee performing the work;

(3) certification of the employee’s security clearance;

(4) period during which the request is to be valid. Visit authorizations shall be renewed, at minimum, every 12 months; and

(5) the contract number.

c. Establish a Security Servicing Agreement that specifies the security functions to be performed by the contractor. Security functions not formally accepted by the contractor remains the responsibility of the command.

d. Include contractor employees in the command’s continuous evaluation program. Commanding officers shall report to the Defense Investigative Service any adverse or questionable information which comes to their attention concerning a cleared contractor employee assigned to a worksite under their control.

e. Ensure the contractor has, or is provided, the necessary equipment to properly safeguard the classified material.

f. Include contractor personnel in the command’s security education program.
1. **Background.** The Naval Warfare Publications Library (NWPL) is the repository for Naval communications and tactical warfare publications. These publications contain required procedures, signals, and other information which are of an operational or mission-essential nature. The NWPL provides for central administration of these publications and for maintenance of those copies which are not distributed to other holders.

2. **Policy.** Commands with an NWPL shall ensure the library is maintained per reference (a) and this instruction. Requests for changes, additions or deletions, to authorized allowances will be made per procedures in this instruction and reference (a).

3. **Responsibilities**
   
a. COMNAVRESFOR (N01A2) will provide the necessary guidance and oversight to ensure commands with an NWPL are aware of proper procedures for maintaining NWP and standardize the organization and administration of the NWPL.

b. Commanding officers will appoint in the command primary/collateral duty notice, a Naval Warfare Publication Custodian (NWPC) who will be responsible for the overall management of the NWPL.

c. The NWP Custodian will:
   
   (1) Maintain all NWPL records,
   
   (2) distribute NWPs and routing information concerning NWPs within the command,
   
   (3) order or produce replacement publications or portions of changes as necessary to maintain complete and current publications,
   
   (4) submit request for allowance changes, and
   
   (5) ensure that classified NWPs are entered into the command’s system of accountability and control and are handled, safeguarded and destroyed per reference (b) and chapters IX, XV and appendix D of this instruction.

4. **Allowance/Automatic Distribution.** The allowance for each NWP, except the NWP 55 series (aircraft tactical manuals), is approved by its Primary Review Authority and maintained by Naval Tactical Support Activity (NTSA). The Primary Review Authority for each publication is listed in appendix A to reference (a). Appendix A provides the current status of the publication (revisions, changes, supplements, errata), and a brief summary of the contents. Distribution of changes and new editions is automatic in quantities specified in the authorized distribution list found in reference (k). The allowance portion of reference (k) is issued on Compact Disk-Read Only Memory (CD-ROM) disk only. Requests for changes (addition/deletion) should be forwarded, via the chain of command, to the Naval Doctrine Command with a copy to NTSA (Code 13). Submit request for changes to CD-ROM distribution to NTSA via Naval Doctrine Command and the chain of command.

5. **NWPL Account Number**
   
a. Any correspondence concerning the NWPL must include the command’s Standard Naval Distribution List (SNDL) (OPNAV P09B2-105 (94)) account number and the command’s Unit Identification Code.
b. Part of a command’s SNDL code is used to create a library account number. The SNDL code is an alphanumeric system using three to five characters and can be found in the SNDL. The SNDL account number for the NWPL will appear in the upper left corner of each page of a command’s publication requirement list.


Commands requesting NATO publications which are classified secret must be designated a NATO Control Point by COMNAVRESFOR (N01A2). Commands requesting NATO publications that are classified restricted and/or confidential need not be designated but must safeguard these publications per the requirements of reference (r) and chapter XV of this instruction.

b. NATO printed copy or microfiche will not be filed or intermingled with those bearing United States classification. If stored in the same container, they must be separated by a distinct division as prescribed in reference (a).

7. Navy Tactical Information Compendium (NTIC)

   a. The NTIC is a suite of CD-ROMs that provides automated access to an extensive and current array of tactical information. The NTIC Series A CD-ROMs provide current information/updates of lessons learned and Fleet Tactical Library documents, as well as other automated databases. NTIC Series B CD-ROMs contain tactical publications currently distributed in printed and microfiche format. Many, but not all NWPs are available on CD-ROM. Initially, all commands on distribution for any of the printed copy contained on the NTIC Series B CD-ROM received a copy of the disks. Modifications of allowance lists will be addressed later as more publications become available on CD-ROM.

   b. The Naval Computer and Telecommunications Command issues communications publications on CD-ROM as part of the NWP system.

   c. Currently, there are no approved methods for destruction of classified CDs. Until such policy is established, all superseded NTIC CDs will be returned to NTIC Distribution using established procedures for transmitting secret material.

8. NWPC. The NWPC is responsible for the management and security of the NWPL. The NWPC should be a Naval officer or responsible chief petty officer or Department of Defense civilian GS5 or above. The NWPC will be designated in writing using the format of figure XVIII-1 of this instruction. If the command issues a primary/collateral duty notice, copy this notice, highlight the name of the appointed personnel and maintain this notice vice a letter. The letter or notice must be updated each time a new custodian/clerk is appointed. An inventory of the NWPL will be conducted when there is a change of custodian/clerk.

9. Administrative File. An administrative file will be maintained which contains copies of all correspondence, in chronological order, relating to naval warfare and communication publications. All documents placed in the administrative file will be kept for at least 2 years unless otherwise noted. The file will be subdivided as follows:

   a. Correspondence File. Correspondence, both internal and external, relating to the NWPL and its publications received or generated by the command will be maintained. This includes memoranda, such as internal requests for publications, changes and message traffic, other than advance change messages.
b. **Local Inventory File.** The inventory sheet is a summary of the current holdings in the NWPL. It lists short title, long title, allowance copies onboard and changes entered (see figure XVIII-2 of this chapter).

c. **Pending Change File.** A Change Entry Certification Form (OPNAV 5070/12) will be made for each change transmitted to a subcustodian of an NWP. Pending and completed forms will be stored in this file.

d. **Publication Notice File.** A local memoranda or route slip will be used to notify cognizant personnel of new publications or changes received onboard. The publication notice is normally incorporated in the front pages of both printed and microfiche publications. The notice can be duplicated for routing to cognizant personnel.

e. **Naval Publication (NAVPUB) Message Checkoff.** NAVPUB Message Checkoff sheets are used to record the review/action on NAVPUB messages relating to the NWPL to ensure no corrections or directives are missed. Messages will be logged in numerical order with a brief description of the subject. Messages that do not pertain to the library will be logged and "no concern" will be annotated in the "subject" column. Reconcile this file against the list of effective messages issued annually. Any message not listed is cancelled. NAVPUB messages may be destroyed after they are cancelled. The 2 year retention for documents in the administration files does not apply to NAVPUB messages.

f. **Access listing.** Maintain an access listing identifying personnel who have been granted access to classified publications and who have been briefed and granted NATO access.

10. **Locator File.** A Library Catalog Card, OPNAV Form 5070/11, (see figure XVIII-3 of this chapter) will be made for each title held on paper, microfiche and each CD series held. The front of the card will list all changes made in the publication and will reflect the same information as the record of changes page in the publication. The reverse of the catalog card is used to record the check out of publications. List the copy number of the publication, name of person checking the publication out, their code/division and date. Upon return of the publication, the custodian/clerk will sign in the "holder" block and indicate "NWPL" in the "location" block.

11. **New Publications.** The initial handling of new publications will depend on whether it is received in printed, microfiche or CD-ROM media.

   a. **Paper copy.** Upon receipt, a new paper copy publication is page checked against the list of effective pages, found at the end of the publication. Record the receipt of the publication on the NWPL inventory/allowance sheet. Complete a Library Catalog Card (OPNAV 5070/11). Reproduce the publication notice and route it to cognizant offices.

   b. **Microfiche.** Upon receipt, a new microfiche is page checked. Annotate the page check in the upper left corner of the microfiche envelope cover. Ensure a Library Catalog Card (OPNAV 5070/11) is completed. Record the receipt on the inventory/allowance sheet. If a microfiche printer is available, print the publication notice and route it. If microfiche reproduction capabilities do not exist, develop a memorandum that will advise cognizant offices of the availability of the publication.

   c. **CD-ROM.** Upon receipt of a new CD-ROM disk, a Library Catalog Card (OPNAV Form 5070/11) will be made for the series (e.g., A1, B1, B2). A separate library card will not be made for each publication on the CD-ROM disk. An NTIC bulletin is provided with each new series released. Route this bulletin to advise cognizant offices of the availability of the new CD-ROM series.
d. Secret NWPs will be entered into the command’s information security accountability program. The control number will be placed on the first paper page on paper and microfiche publications. An adhesive label containing the control number will be placed on the back left top corner of the CD case. Secret CD-ROM disks have a unique serial number located in the center of the disk. This number should be used to identify and control the disk.

12. Changes. When an NWP change or correction (printed or message) is received, the custodian/clerk will conduct a page check of the change to ensure completeness. If the check reveals an incomplete change or correction, a report will be made per reference (a), chapter 4, and a replacement copy ordered.

   a. Make pen and ink entries in any dark ink, except red.

   b. Enter the change when it is effective. Check for an effective date by reading the letter of promulgation or forward letter. If the change is awaiting a NATO effective date, safeguard the change per its classification.

   c. Annotate the change on the Library Catalog Card (OPNAV 5070/11), record of changes page and on the inventory/allowance sheet after it has become effective.

   d. After the change is entered and before the residue is destroyed, make a page check of the publication against the list of effective pages and annotate the page check on the record of change page.

   e. If the change or correction is to a publication that is checked out, recall the publication and enter the change as provided above, or cause the change to be entered as follows:

      (1) Fill out the first line of part 1 and part 2 of a Change Entry Certification (OPNAV 5070/12) and attach it to the change or correction.

      (2) Transmit the change or correction to the subcustodian with the OPNAV 5070/12 attached on or before the effective date of the change or correction.

      (3) Obtain the signature of the subcustodian and the date of receipt on the bottom of part 1 of the OPNAV 5070/12. Part 1 is detached and kept in the administrative file to serve as a tickler for the change. Part 2 is kept by the subcustodian. The subcustodian must make the change entry on the effective date. After the subcustodian has entered the change, part 2 will be completed and returned within 5 days to the NWPL custodian together with any change residue. The custodian will annotate the appropriate catalog card and inventory/allowance sheet with the change and destroy part 1 previously used as a tickler. Part 2 of the form is kept in the administrative file for 2 years.

13. Microfiche Changes. A 3 x 5 inch card will be inserted in the envelope of each copy of microfiche that has received a message correction with the words “See Change Folder” printed thereon. A separate folder will be maintained for each microfiche with corrections. The change folder will have message corrections in numerical order. The corrections will be kept until an updated microfiche is received. The corrections will be destroyed when the microfiche is destroyed. Make sure all corrections are annotated on the front of the library catalog card and on the front of the microfiche envelope.

14. Ordering Publications/Changes. A full Military Standard Requisitioning and Issue Procedures (DD Form 1348), in message format, must be submitted to Navy Aviation Supply Office, Cog I for all publications ordered. NSN for publications can be found in the NWPSSTAT file on disk 1 of series B1 of the CD-ROMs. General assistance with publications, directives, and forms should
be addressed to the Customer Service Section of Aviation Supply Office at DSN 442-2660 or commercial (215) 697-2660.

15. Inventories/Inspections. NWPLs will be inspected at least annually by a cleared individual senior to the custodian. A complete inventory of publications will be conducted with the inspection. A letter detailing the results of the inspection/inventory will be provided to the commanding officer with a copy to the custodian. The custodian will provide to the commanding officer, within 30 days, a listing of corrective actions taken with regard to deficiencies noted. A copy of the inspection/inventory will be retained in the administrative file for 2 years. An inventory of the NWPL will also be conducted when there is a change of custodian/clerk or change of command.
From: Commanding Officer
To: (Person being designated as Naval Warfare Publications Custodian)

Subj: DESIGNATION AS NAVAL WARFARE PUBLICATIONS CUSTODIAN

Ref: (a) NWP 1-01
     (b) NTP 4
     (c) OPNAVINST 5510.1H
     (d) OPNAVINST 3120.32B
     (e) COMNAVRESFORINST 5500.3A

1. Per reference (a), you are hereby designated as the Naval Warfare Publications Custodian for this command. Your responsibilities and duties are in references (a) through (e).

2. Further, you are directed to conduct a complete inventory of the command’s Naval Warfare Publication Library and submit a report of findings prior to assuming the duties of custodian.

__________________________________________________________
(Commanding Officer)

From: (Designated Custodian)  
To: Commanding Officer, ______________________

Subj: NAVAL WARFARE PUBLICATIONS INVENTORY

Ref: (a) Commanding Officer ______ ltr Ser ______ of

1. Per reference (a), an inventory of all publications and a review of administrative records and files of the Naval Warfare Publication Library was conducted on (date). The inventory revealed (no discrepancies) (the following discrepancies which have subsequently been corrected:

   a. (list discrepancies))

2. I hereby relieve (name of present custodian) as the Naval Warfare Publications Custodian.

__________________________________________________________
(Signature of Relieving Custodian)

Figure XVIII-1

XVIII-6
INVENTORY/ALLOWANCE SHEET

11 MAY 1995

RECOMMENDATIONS:

1. Short and long titles typed on to sheet.
2. Remarks and publication suffix written with pencil.
3. Remarks column used to show latest change or correction entered for that publication.
4. Update allowance and onboard lists:
   (a) Upon receipt of new publication
   (b) Upon receipt of new allowance list (OPNAVINST 5605.19J)
   (c) When any change occurs to library
5. Keep Inventory/Allowance sheet as accurate as possible.

Figure XVIII-2

NWPL Catalog Card

* ENTRY DATE will be written into each column for each publication receiving change or correction.

Figure VXIII-3 (Front)

XVIII-7
**COMNAVRESFORINST 5500.3A CH-1**

**11 MAY 1995**

**OPNAV 5070/11 (Rev: 9.75) BACK**

### DISPOSITION OF PUBLICATION

<table>
<thead>
<tr>
<th>COPY NO.</th>
<th>HOLDER (Signature)</th>
<th>LOCATION</th>
<th>REC'D DATE</th>
<th>RETURN DATE</th>
<th>DESTRUCTION DATE</th>
<th>AUTHORITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>142</td>
<td>NWPL Custodian's Sig</td>
<td>NWPL</td>
<td>*1</td>
<td>*5</td>
<td>*6</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Subcustodian's Sig</td>
<td>OPS</td>
<td>*2</td>
<td>*3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>NWPL Custodian's Sig</td>
<td>NWPL</td>
<td>*4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTES:**

*1. Date copy received into library.*
*2. Date subcustodian received copy.*
*3. Date subcustodian returns copy to library.*
*4. Date publication received by library.*
*5. Date copy destroyed.*
*6. Authority cited for destruction of copy.*

Figure XVIII-3 (Back)
# Table of Contents

Letter of Issuance  
Cross Reference (Locator) sheet  
Record of Changes  
Table of Contents

I. Program Management  
II. Base/Shore Facilities Physical Security  
III. Shore Activities Physical Security Plans  
IV. Security Forces  
V. Auxiliary Security Forces (ASF)  
VI. Security Education  
VII. Security of Sensitive Conventional Arms, Ammunition and Explosives  
VIII. Threat/Security Conditions  
IX. Information and Personnel Security  
X. Loss Prevention  
XI. Law Enforcement/Security Office Forms  
XII. Bomb Threats  
XIII. Flightline Physical Security  
XIV. Crime Prevention  
XV. Safeguarding North Atlantic Treaty Organization (NATO) Classified Materials  
XVI. Industrial Security  
XVII. Combating Terrorism  
XVIII. Naval Warfare Publications (NWP)  
XIX. Violence in the Workplace

APPENDIX A  
Course of Instruction – Auxiliary Security Force (ASF)  
APPENDIX B  
Bomb Threats  
APPENDIX C  
Part 1-Flightline Physical Security  
Part 2-Minimum Flightline Physical Security Standards  
Part 3-Tenant Activity Support Responsibilities  
Part 4-Flightline Personnel Control Procedures  
Part 5-Flightline/Support Facility Badges  
Part 6-Flightline Vehicle Control Procedures  
APPENDIX D  
Accountability and Control of Classified Material  
APPENDIX E  
Part 1–NATO Classified Material Briefing Guide  
Part 2–NATO Inspection Checklist  
APPENDIX F  
Lesson Topic Guide
CHAPTER XIX

VIOLENCE IN THE WORKPLACE

1. **Background.** Violence in the workplace is a growing phenomenon. Workplace homicide is on the rise, and our installations are not immune. Actions by disgruntled individuals, due to economic, social, and cultural pressures, impacts individuals, organizations, and communities. Violence in the workplace is a threat to force protection, our people, resources and our missions.

2. **Policy.** Command emphasis and a civilian/military leader’s attention to causative factors of violence and intervention are essential to minimize the effects on the work force. Commanding officers will develop strategies to identify situations conducive to violence and implement measures to reduce the occurrence of violence.

3. **Responsibilities.** Commanding officers will reduce the risk of violence in the workplace through a combination of awareness, education, open communications, and employee support services.
   a. **Awareness.** Commands will identify potential stress inducing policies or procedures and implement intervention strategies.
   b. **Education.** Civilian and military leaders will incorporate sequential and progressive awareness training into existing professional development courses. Leaders should:
      (1) Ensure all military and civilian supervisors complete appropriate training such as the Navy Leadership Education and Development course.
      (2) Include coverage of local policies and procedures on violent or disruptive behavior in new employee orientation programs.
      (3) Educate the work force on available resources and services to assist individuals with personal problems which may impact performance or behavior.
      (4) Design specific short-term training sessions to address work force issues which could contribute to stress in the work force.
      (5) Consider the use of stress management training.
   c. **Open Communications.** Leaders play a critical role in reducing the risk of violence and protecting the work force. Employees must be able to air grievances and report potential violent activity within their respective work places. Open communications can only be successful within an environment free of reprisal. Leaders and supervisors must be responsive to employee concerns and establish a responsive system providing feedback. Keys to success are:
      (1) An active and vibrant command information program.
      (2) Early, candid, and continuing communications on actions affecting employment security.
      (3) Leaders/supervisors’ use of mentoring, counseling, and coaching techniques to gain employee trust and facilitate communications on matters of concern to them.
   d. **Employee Support Services.** Within an installation, support services organizations can assist employees in managing stress that may affect the
workplace. Integrate services into the strategy to reduce the risk of violence. The following list includes types of support services that may be available and that may assist in reducing/avoiding workplace violence:

1. **Family Service Center/Family Advocacy Program**
   - (a) Provides installation alcohol and drug abuse/awareness program which includes prevention, education, and suicide prevention.
   - (b) Provides advocacy and outreach services.
   - (c) Provides command statistical data on reported violence involving child and spousal abuse.
   - (d) Provides family violence awareness, prevention skills, and intervention training.
   - (e) Provides response to incidents of violence in the workplace and ensures referrals and appropriate follow up.

2. **Chaplain**
   - (a) Provides spiritual, moral, and religious support.
   - (b) Provides marriage and family counseling, and other services that promote inner stability, calm, and peace.
   - (c) Provides the command with a command “pulse” on quality of life, perceptions, and indications of changing climates.

3. **Public Affairs Officer**
   - (a) Advises the commanding officer on public affairs issues related to violence in the workplace.
   - (b) Develops a command information plan to increase awareness of available assistance and on issues relating to violence in the workplace.
   - (c) Publishes articles in local publications in concert with local subject matter experts.

4. **Security officer**
   - (a) Reports incidents of violence to the supporting Naval Criminal Investigative Service.
   - (b) Records critical information (who, what, where, and how) on incidents.
   - (c) Provides an installation Special Reaction Team or establishes an agreement with local police authorities—who are capable of providing a response to developed threats (i.e., hostage situation, violent acts).

5. **Human Resources Office**
   - (a) Assists in arranging for training related to stress management and dealing with problem employees.
   - (b) Assists management in ensuring personnel actions are executed in a caring and sensitive manner.
(c) Assists management in promoting innovative work arrangements such as flextime, compressed and alternate work schedules, and job sharing.

(d) Provides guidance to activities and individuals on the availability of short-term counseling and referral services under the Civilian Employee Assistance Program.

(6) **Equal Employment Office**

(a) Assists commanding officers in providing an environment free of discrimination based on race, sex, age, religion, color, national origin, reprisal, and physical and mental handicap.

(b) Assists with the resolution of complaints focusing on underlying issues.

(c) Provides statistical data on policies and systemic organizational issues affecting complaints of discrimination.

(7) **Safety Officer**

(a) Assists leaders in establishing a command climate which is sensitive and responsive to factors contributing to workplace violence.

(b) Reviews "human error" causal elements which may identify worker stress or negative environmental or ergonomic factors.

(c) Assists in assessing the physical and social environment for potential negative and positive stressors (e.g., space, lighting, temperature, equipment, noise level).

(d) Continues efforts to identify deficiencies that would negatively impact a safe and healthful workplace.

(8) **Judge Advocate General Corps/Legal Officer**

(a) Provides legal assistance services to eligible personnel on personal legal problems of a civil nature such as nonsupport, indebtedness, and separation/divorce.

(b) Provides legal advice to commanding officers concerning the disposition of violent misconduct that occurs in the federal workplace.
Subj: COMMANDER, NAVAL RESERVE FORCE (COMNAVRESFOR) SECURITY MANUAL

Ref: 
(a) SECNAVINST 5820.7B (Cooperation with Civilian Law Enforcement Officials)
(b) OPNAVINST 5510.1H (Department of the Navy Information and Personnel Security Program Regulation)
(c) OPNAVINST 5530.14B (Department of the Navy Physical Security and Loss Prevention Manual)
(d) OPNAVINST 5530.15 (Physical Security Joint Services Pub)
(e) SECNAVINST 5530.4A (Naval Security Forces Ashore and Afloat)
(f) OPNAVINST 5580.1 (Naval Law Enforcement Manual)
(g) NAVOP 028/92 (Weapons and Violence)
(h) OPNAVINST 11010.20E (Facilities Projects Manual)
(i) SECNAVINST 5511.36A (Authority of Military Commanders under the Internal Security Act of 1950 to Issue Security Orders and Regulations for the Protection of Property and Places under their Command)
(j) COMNAVAIRESFORINST 5720.11A (Commander, Naval Air Reserve Force Sponsored Air Show/Open House Events, Policy Guidance)
(k) SECNAVINST 5500.32B (Carrying of Firearms by Personnel of the Department of the Navy)
(l) SECNAVINST 5500.29B (Use of Force by Personnel Engaged in Law Enforcement and Security Duties)
(m) OPNAVINST 1020.4A (Standard for Wearing Camouflage Utility Uniform by Navy Security Force Personnel)
(n) OPNAVINST 5530.13A (Department of the Navy Physical Security Instruction for Sensitive Conventional Arms, Ammunition and Explosives (AA&E))
(o) NAVSEAINST 8370.2 (Small Arms and Weapons Management Policy and Guidance Manual)
(p) SECNAVINST 5500.4F (Reporting of Missing, Lost, Stolen, or Recovered Government Property)
(q) SECNAVINST 5500.31A (Technical Surveillance Countermeasures (TSCM) Program)
(r) OPNAVINST C5510.101D (NATO Security Procedures (NOTAL))
(s) OPNAVINST 3300.53 (Navy Combating Terrorism Program)

1. **Purpose.** To consolidate existing Department of the Navy and COMNAVRESFOR instructions on security and related regulations/publications into one document for the management and coordination of Reserve-wide Navy security programs and to implement the Navy’s security programs within COMNAVRESFOR’s claimancy. This includes policy, guidance, and assignment of responsibilities for the security of personnel, property, information, and material assigned to the Naval Reserve. This instruction has major revisions incorporated and should be read in its entirety.
2. **Cancellation.** COMNAVRESFORINST 5500.3, COMNAVRESFORINST 5510.6, and COMNAVRESFORINST 5820.1.

3. **Scope.** COMNAVRESFOR’s emphasis on security extends to all Naval Reserve commands, and applies equally to all active and inactive duty military, and civilian personnel assigned to or associated through employment with the COMNAVRESFOR claimancy.

4. **Action.** All echelons of command shall establish security programs commensurate with their needs, using references (a) through (s) and this instruction for guidance.

5. **Forms**

   a. The following forms are available through normal Navy supply channels per NAVSUP P2002D using the National Stock Numbers (NSNs) cited:

      | Form Description                              | NSN                |
      |----------------------------------------------|--------------------|
      | Authorization to Carry Firearm                | 0107-LF-055-1400   |
      | Non-Government Vehicle Registration          | 0701-LF-055-6005   |
      | Personnel Security Action Request            | 0107-LF-009-4200   |
      | Visitor and Vehicle Registration Log         | 0117-LF-055-3205   |
      | Record of Disclosure                         | 0107-LF-055-1165   |
      | Telephonic Threat Complaint                  | 0107-LF-055-2740   |
      | Record of Receipt                            | 0107-LF-008-8000   |

   b. CNET-GEN 5512/3 and 5512/8 may be obtained by submitting, through your supply system, a DD-1348 to Commanding Officer, Navy Supply Center (Code 101.3), Naval Air Station, Pensacola, FL 32508-6200:

      | Form Description                          | NSN                |
      |-------------------------------------------|--------------------|
      | Pass Application                          | 0197-LL-NF3-1341   |
      | Temporary Vehicle Pass                    | 0197-LL-NF3-1391   |

   c. Optional Form 55 may be obtained from the General Services Administration:
OPTIONAL FORM 55

U.S. Government Identification

The following forms may be obtained by submitting a memorandum to COMNAVRESFOR (Code 01A2), 4400 Dauphine St., New Orleans; LA 70146-5046:

NAVRES 5580/1

Deadly Force Certification

DAAG Form 29

Subregistry/Control Point Signature List

e. The NAVRES 5511/5 (Classified Material Control Form) is a computer generated form.

6. Reports

The NATO Annual Inspection/Inventory requirement contained in paragraph 5 of Chapter 15 has been assigned report symbol COMNAVRESFOR 5510-2. This requirement will remain in effect for three years from the date of this directive.

b. The requirement for DoD Support to Civilian Law Enforcement Officials contained in paragraph 3 of Chapter 16 has been assigned report symbol OPNAV 5820-1 per reference (a).

c. The requirement to report incidents of possible compromise or actual compromise contained in paragraph 4a(6)(e) of Chapter 15 has been assigned report symbol OPNAV 5510-6B per reference (b).

Distribution: (COMNAVRESFORINST 5216.1H)
List B
- C1 (26R1, 26R2, 28C1, only)
- C2 (less 39B1, 39B2, 39C1, 39C2, 39E1)
- D
- E2 (26WIA and 26TTT only)
- F2 (PERSUPPDET NAS New Orleans, PERSUPPDET NAVSUPPACT New Orleans only)

Copy to: (COMNAVRESFORINST 5216.1H)
List A (A3 (CNO (N-095) only))
- E1 (21A1, 21A2 only)
- E9 (45B, V6 only)

Stocked:
COMNAVRESFOR (Code 01A)
<table>
<thead>
<tr>
<th><strong>DIRECTIVE:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>DATE OF DIRECTIVE:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SUBJECT:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SEE:</strong> (where publication is maintained)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>REMARKS:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Signature of Receipt</strong></th>
<th><strong>Date</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### RECORD OF CHANGES

<table>
<thead>
<tr>
<th>CHANGES NO.</th>
<th>DATE RECEIVED</th>
<th>DATE ENTERED</th>
<th>BY WHOM ENTERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

Letter of Issuance i
Cross Reference (Locator) sheet unnumbered
Record of Changes i
Table of Contents iii

I. Program Management I-1
II. Base/Shore Facilities Physical Security II-1
III. Shore Activities Physical Security Plans III-1
IV. Security Forces IV-1
V. Auxiliary Security Forces (ASF) V-1
VI. Security Education VI-1
VII. Security of Sensitive Conventional Arms, Ammunition and Explosives VII-1
VIII. Threat/Security Conditions VIII-1
IX. Information and Personnel Security IX-1
x. Loss Prevention X-1
XI. Law Enforcement/Security Office Forms XI-1
XII. Bomb Threats XII-1
XIII. Flightline Physical Security XIII-1
XIV. Crime Prevention XIV-1
XI. Safeguarding North Atlantic Treaty Organization (NATO) Classified Materials XV-1
XVI. Reporting Requirements for Support to Civilian Law Enforcement Officials XVI-1
XVII. Combating Terrorism XVII-1

APPENDIX A A-1
Course of Instruction - Auxiliary Security Force (ASF) A-1

APPENDIX B B-1
Bomb Threats B-1

APPENDIX C C-1
Part 1-Flightline Physical Security C-1
Part 2-Minimum Flightline Physical Security Standards C-2
Part 3-Tenant Activity Support Responsibilities C-4
Part 4-Flightline Personnel Control Procedures C-5
Part 5-Flightline/Support Facility Badges C-6
Part 6-Flightline Vehicle Control Procedures C-10
CHAPTER I

PROGRAM MANAGEMENT

1. Background. References (c) and (d) require all Navy shore-based activities to establish and maintain effective and comprehensive security programs. To be effective, security programs must receive command attention and direction, and functions must be carried out by properly trained and equipped personnel.

2. Policy. All subordinate commands will ensure that security is given the attention necessary to effectively protect personnel, assets, and facilities against all threats, internal and external, which could impact the mission of the activity or reduce readiness. Maintaining high standards of security is an item of primary importance at all levels of command.

3. Responsibilities. The following personnel will be responsible for the management and coordination of security programs within the COMNAVRESFOR area of responsibility.

   a. COMNAVRESFOR - The Security Officer (Code 01A2) will develop policy, manage, and coordinate security programs for COMNAVRESFOR. Coordination of program requirements will be made with the following codes:

      (1) Deputy Chief of Staff Financial Management (Code 06) for programing funds.

      (2) Deputy Chief of Staff for Facilities (Code 08) for coordinating security improvement projects of bases/facilities.

      (3) COMNAVRESFOR Inspector General (Code 002) for the conduct of security inspections.

   b. Echelon III, IV, and V commands (except Naval Reserve augmentation units) - Commanding officers are responsible for security within their commands. Per references (b) and (c), commanding officers will designate a security officer and a security manager in writing, and ensure they are provided sufficient training, resources, staff assistance, and authority to manage and carry out effective security programs. The security officer and security manager will report directly to the commanding officer, or via the executive officer to the commanding officer. One individual may be assigned both functions if workload permits.

      (1) The security officer is responsible for implementing the provisions of references (c) and (d) and all other current security directives. The security officer shall determine the adequacy of security programs, identify those areas in which improvements are required, provide recommendations for such improvements and shall:
(a) conduct inspections of subordinate activities to ensure the adequacy of their security programs and provide assistance and resources for correcting deficiencies,

(b) develop and maintain a current command physical security plan,

(c) conduct physical security surveys, inspections, and audits,

(d) determine and identify the necessary resources (i.e., funds, staff, equipment) to implement an effective security program,

(e) coordinate security requirements of tenant activities and ensure that their requirements are entered in applicable inter/intra-service support agreements,

(f) develop written physical security instructions to cover all phases of security operations,

(g) submit, via the chain of command, requests for waivers or exceptions when the security standards of references (c), (d), and (e) are not being met. Initial request for waivers will be evaluated and approved or disapproved by COMNAVRESFOR (Code 01A2). Requests for extensions of waivers, and all requests for exceptions, will be addressed to Chief of Naval Operations (CNO) (N-09N1) via the chain of command,

(h) coordinate with the command substance abuse coordinator on the use of drug detector dogs. Ensure semiannual sweeps are conducted which will include one drill weekend, and

(i) ensure the requirements of references (f) and (g) are enforced and that the unauthorized possession of weapons is addressed at all levels of training.

(2) The security manager serves as the commanding officer’s advisor and direct representative in matters pertaining to the information and personnel security program and is responsible for the management of the program per reference (b). The security manager shall:

(a) conduct inspections of subordinate activities to ensure the adequacy of their information and personnel security programs and assist in correcting deficiencies,

(b) develop written command information and personnel security procedures, including an emergency plan,

(c) formulate and coordinate an information security education program,
(d) ensure compliance with the requirements of reference (b) for the receipt, handling, storage, accountability, and destruction of classified materials,

(e) formulate and coordinate with the security officer the physical security measures for protection of classified material,

(f) ensure personnel security investigations, clearances, and access are recorded and monitored, and

(g) submit, via the chain of command, requests for waivers or exceptions when the security standards of reference (b) are not being met. Initial requests for waivers will be evaluated and approved or disapproved by COMNAVRESFOR (Code 01A2). Requests for extensions of waivers, and all requests for exceptions, will be addressed to CNO (N-09N2) via the chain of command.

(3) Tenant activities will coordinate their appropriate security needs with the host activity security office and ensure compliance with all host activity security requirements. Such compliance does not relieve Naval Reserve commands from having their own internal security programs per references (b) and (c). Requirements include, but are not limited to, the following and those contained in other chapters of this instruction:

(a) written procedures/regulations covering all phases of security and security plans for both physical and information/personnel security, including normal and emergency situations,

(b) good working relationship with the host command security office and/or local law enforcement agencies, as applicable. Inter/intra service support agreements on security will be in effect for commands that are tenants on major military installations,

(c) a security officer/security manager designated in writing by the commanding officer and identified by name on organization charts, telephone listings, collaterals duty lists, and building directories,

(d) a strict key and lock control program managed and supervised by the security officer,

(e) procedures for identifying and controlling personnel and vehicle access,

(f) an annual security survey, and

(g) designation of restricted areas in writing, including minimum security measures to ensure adequate protection of the area.
(h) Provide indoctrination and annual refresher briefings in both physical and information/personnel security as required by references (b) and (c).

c. Naval Criminal Investigative Service Command’s Anti-terrorist Alert Center will provide intelligence analysis of the terrorist/unconventional warfare threats and disseminate warning reports as required.
CHAPTER II

BASE/SHORE FACILITIES PHYSICAL SECURITY

1. **Background.** References (c) and (d) establish minimum physical security standards for U.S. Navy bases/shore facilities. The application of these standards is influenced by the mission of the activity, the type and jurisdiction of the property, the geographic location and size of the activity, the topography of the area, the economic and political atmosphere, potential and existing threats and the logistical and operational support given to these factors in establishing activity security requirements.

2. **Policy.** Commands will continuously assess their security posture, identify weaknesses and determine corrective measures to ensure compliance with the standards of references (c) and (d). Annual physical security surveys will be conducted to establish priorities for funding/work accomplishment.

3. **Responsibilities**
   
   a. Commanding officers will ensure compliance with references (c) and (d) and effectively monitor security requirements to ensure they receive appropriate attention consistent with local threats and conditions.

   b. Commands shall develop local directives/orders that cover all phases of security operations.

   c. Commands will conduct annual physical security surveys to include a complete reconnaissance, study, and analysis of the physical security posture of the installation and its operations.

   d. COMNAVRESFOR (Code 01A2) will review all major security issues and problems encountered by Naval Reserve commands and recommend courses of action.

   e. Deputy Chief of Staff (Code 08) will coordinate all special and military construction Naval Reserve security improvement projects with the security officer. Reserve activities will submit request for special security projects as follows:

   (1) facility security projects exceeding the commanding officer’s funding authority will be submitted per reference (h),

   (2) in preparing the projects, both Step I and Step II submissions should identify and provide cost estimates for any Other Procurement Navy or expense type equipment items (intrusion detection systems; closed circuit television). Although these costs are not part of the project cost, advance budgeting by the activity will be required for this equipment,
(3) as required in all project preparation, care should be taken to identify and show costs of repair and construction items in combined projects, and

(4) the activity commanding officer shall ensure that physical security issues are discussed and addressed during the preparation of the activity master plan.

f. Deputy Chief of Staff (Code 06) will coordinate funding requirements for security related items with the Deputy Chief of Staff (Code 08) and the Security Officer (Code 01A2) to ensure adequate and timely budget submissions.

g. COMNAVRESFOR (Code 01A2) will coordinate with the Deputy Chief of Staff (Code 02) to facilitate adequate billet programming and manning priorities.

h. Commands shall ensure that security requirements are coordinated between individual command managers and the financial management staff, and are submitted per the Navy’s planning, programming, and budgeting system.
CHAPTER III

SHORE ACTIVITIES PHYSICAL SECURITY PLANS

1. **Background.** References (c) and (d) require each naval shore activity/installation to develop and publish a physical security plan which issues standard operating procedures for day-to-day security operations as well as crisis management. Reference (i) authorizes the issuance of security orders and regulations for the protection and security of installations and their assets.

2. **Policy.** All Echelon III, IV, and V commands (except Naval Reserve augmentation units) shall develop and publish a physical security plan per reference (c).

3. **Responsibilities**
   
   a. Commanding officers will ensure that a physical security plan is developed and published to cover all phases of security operations and that periodic reviews are made to ensure the currency of the plan.
   
   b. Command security officers should develop and maintain a current physical security plan which, at a minimum, addresses the following security interests.

      (1) Restricted areas - Designate areas, buildings, and other structures considered critical, and establish priorities for their protection.

      (2) Personnel and vehicle access - Establish controls for ingress and egress to each area, and assign systems for identification and control.

      (3) Security aids - Indicate the various types of security aids (i.e., protective barriers, signs, gates, lighting, intrusion detection systems, and communications systems) to be used, and develop policy for use on the installation.

      (4) Security forces - Develop policy and standard operating procedures for the security force to include special and general orders for each post. Policy relating to the staffing, training, and deployment of an auxiliary security force shall be included.

      (5) Crisis management - Indicate required action in response to various emergency situations, i.e., fires, explosions, civil disturbances, major accidents, hostage situations, sabotage, bomb threat incidents, terrorist acts, natural disasters, and other potential crises as appropriate.

   c. The Naval Criminal Investigative Service Resident Agent will supply an area threat assessment for commands upon request. Threat assessments should be used to update and revise security plans based on local threat conditions.
The COMNAVRESFOR Security Office will provide assistance to subordinate activities in the development of security plans and will provide up-to-date information on state-of-the-art security equipment and methods. A generic physical security plan, with emergency response annexes, is available from COMNAVRESFOR (01A2) upon request.

Physical Security Plans at Naval Reserve air stations/facilities will address security requirements during air shows/open house events per the requirements outlined in reference (j) and chapter 13 of this instruction.
CHAPTER IV

SECURITY FORCES

1. **Background.** The Navy Security Force (NSF) constitutes one of the most important elements of an activity’s security program. It provides the enforcement and implementation medium of the security effort. Properly used, it is one of the commander’s most effective and useful tools in a comprehensive, integrated physical security program.

2. **Policy.** Naval Air Stations, Naval Air Facilities and the Naval Support Activity New Orleans shall establish, train, and equip a security force to ensure the proper protection of Navy resources against terrorist, criminal, and enemy actions which could impair the mission of the command or reduce its effectiveness.

3. **Responsibilities**
   
a. COMNAVRESFOR Deputy Chief of Staff (Code 02) shall ensure all military management policies, procedures, and current manning documents guide the assignment of appropriately trained/rated security personnel to Reserve commands.

   b. COMNAVRESFOR (Code 01A2) will ensure that deficiencies in security force manning are brought to the attention of higher authorities and that full support for reducing shortfalls is provided by COMNAVRESFOR.

   c. Commanding officers will ensure that security forces are established, trained, and equipped to provide a degree of protection commensurate with the local threat(s), and will ensure:

      (1) Security force personnel are armed with a loaded weapon when on duty and have in their possession a signed OPNAV Form 5512/2 (Rev 6-81) (Authorization to Carry Firearm).

      (2) The command security officer is trained prior to assuming his/her duties. At a minimum, the security officer must attend the Physical Security and Law Enforcement Supervisor’s Course within three months of appointment.

      (3) Security functions are organized as a department per references (c) and (f), and enclosure (6) to reference (e).

   d. Command security officers are responsible for:

      (1) Organizing, supervising, and training the NSF.
(2) Identifying the number of posts and patrols required to protect against situations and circumstances which threaten personnel and property.

(3) Establishing and maintaining post orders, standard operating procedures, and training for the NSF and auxiliary security force.

(4) Ensuring all security force personnel are properly trained and qualified with their assigned weapons and equipment per references (c) and (k) and receive regular briefings on the use of deadly force as required by reference (l). NSF and auxiliary security forces are not authorized to train with or use M14 and/or M16 rifles in the performance of their duties.

(5) Ensuring personnel are provided training per reference (c) and that funds are budgeted for personnel to attend the Navy Security Guard Training Course, if not attended while enroute on permanent change of station orders. Ensure frequent reinforcement training is provided to emphasize and enhance skills previously learned. All training, including firearms and use of deadly force, will be documented as outlined in references (c) and (l). Deadly force training will be documented using NAVRES 5580/11 (Deadly Force Certification) .

(6) Ensuring security force operations are conducted per reference (f).

(7) Ensuring security force personnel are taught to employ their technical proficiency with other team members to operate as part of a team.

(8) Ensuring security force personnel are provided camouflage utility uniforms as their standard uniform and the uniform is worn as prescribed in enclosure (1) to reference (m).

(9) Ensuring security force vehicles meet the standards and are inspected per references (c) and (f); and security force personnel who operate a vehicle are trained in emergency vehicle operations per the Department of Transportation, National Highway Traffic Safety Administration an reference (f) requirements.

(10) Ensure an effective evidence custody program is established per chapter 17 of reference (f).
CHAPTER V

AUXILIARY SECURITY FORCES (ASF)

1. **Background.** Security force organizations are staffed to provide day-to-day response to the activity’s law enforcement and physical security needs. Augmentation to respond to crisis situations and increased security threats will be necessary. Therefore, a well-trained and equipped ASF is an essential part of the security program.

2. **Policy.** Commands with an NSF shall organize, equip, and train an ASF to support the installation’s permanent security force in times of increased security threat or emergency conditions. ASF composition will be based on military population, using permanently assigned military personnel from host and tenant activities. The ASF will be sized by determining the number of posts needed to implement Threat Condition (THREATCON) Delta security measures and sustain that security posture for at least five days.

3. **Responsibilities**

   a. Commanding officers shall ensure that an ASF is organized, trained, and equipped to respond to increased security threats and other emergency situations.

   b. Tenant activities will provide personnel as required, by the host activity, to staff an ASF and will allow adequate exercising of the force. All personnel selected will meet Navy standards for weight and pass the physical fitness test prior to being assigned; have no drug or alcohol dependency; be mature with sound judgment and have no non-judicial punishment/civil or court martial convictions in the previous two years.

   c. Commanding officers and command security officers will ensure that ASF personnel are assigned only to appropriate duties as specified in reference (m).

   d. The command security officer assisted by a Marine Corps Cadre assigned to the security department, or a mobile training team, will train ASF personnel per Appendix A of this instruction and is responsible for:

      (1) supervision and scheduling of the ASF training program,

      (2) establishing and maintaining individual training records,

      (3) providing training facilities, supplies, and equipment,

      (4) certification of ASF members’ authorization to perform specified duties,
(5) furnishing special expertise instructors and assistant instructors to augment/assist the Marine Corps Cadre as needed, and

(6) prepare lesson plans to support any special subjects unique to the installation.
CHAPTER VI
SECURITY EDUCATION

1. **Background.** Any security program or system designed to combat a threat will prove ineffective unless it is supported by security education. Security consciousness and awareness must be stressed through a continuous, vigorous, and forceful security education program.

2. **Policy.** Commands will develop and implement a comprehensive security education program that will ensure all assigned personnel, military and civilian, recognize, understand, and carry out their responsibilities regarding security. These programs will be tailored to the particular circumstances of each activity and will consist of the following:

   a. General military training of all personnel in both information and physical security,
   
   b. a security indoctrination for all newly assigned personnel which stresses the need for and dangers to security, and
   
   c. specialized training for personnel directly involved in the accomplishment of security/law enforcement duties.

3. **Responsibilities**

   a. COMNAVRESFOR (Code 01A2) will ensure that activities are provided up-to-date information on security education and course availability. A compendium of reference materials on law enforcement, physical security, anti-terrorism, low intensity conflict, and crime prevention will be provided upon request.

   b. Commanding officers will give special attention to security education programs and ensure they meet the needs of the command.

   c. Command security officers/managers should have primary responsibility for implementing the security education program and ensuring maximum participation at their commands.

   d. Command training officers shall provide maximum assistance and support to the security officers in carrying out training responsibilities by coordinating training schedules, classroom facilities and equipment, and by providing information on the availability of training resources.

4. **Anti-terrorist training.** Training for Navy security force and auxiliary security force personnel shall include specific anti-terrorist training, to include scenarios which are consistent with current and potential threats facing an installation, entry control procedures, identification media, preplanned scenario drills, condition simulations, and field exercises.
5. **Weapons and Violence.** Commanding officers shall ensure that unauthorized possession/use of dangerous and illegal weapons is addressed at all levels of training, including accession points and regularly scheduled command general military training. This will heighten awareness and ensure that personnel thoroughly understand and fully comply with the requirements of references (c), (f), and (g).
CHAPTER VII

SECURITY OF SENSITIVE CONVENTIONAL ARMS, AMMUNITION, AND EXPLOSIVES (AA&E)

1. Background The acquisition of AA&E worldwide has been recognized as a prerequisite for the continued operations of violence-oriented terrorist organizations and highly organized criminal elements. Stocks of AA&E in magazines, armories and arms rooms; disaffected military and civilian employees; and M&E shipments via commercial and military modes are lucrative sources for obtaining quantities of AA&E which have highly destructive capabilities.

2. Policy. All commands which hold, process, repair, use, and/or store AA&E shall comply with all security and accountability requirements per references (n) and (o).

3. Responsibilities

   COMNAVRESFOR (Code 01A2) shall coordinate with COMNAVRESFOR Deputy Chief of Staff (Code 08) and COMNAVAIRESFOR (Code 517) on the necessary security improvement projects for protection of AA&E.

   b. Commanding officers of activities shall ensure that:

      (1) quantities of AA&E in the custody of operational units are held to the minimum level consistent with operational, safety, and training requirements,

      (2) the security standards of reference (n) are met or, if meeting such standards is not feasible, that compensatory measures providing equivalent protection are effected,

      (3) waiver and/or exception requests are submitted where the standards of reference (n) cannot be met,

      (4) the command physical security plan specifically addresses the security of AA&E storage sites and provides for adequate, timely response to threats,

      (5) an effective key and lock control program exists for all keys, locks, and lock combinations to AA&E storage areas,

      (6) an AA&E accountability officer is designated in writing with responsibility to monitor all AA&E accountability matters, and

      (7) losses of AA&E are reported immediately per references (n) and (P). In-depth investigations must be initiated to determine the circumstances and assign responsibility.
CHAPTER VIII
THREAT/SECURITY CONDITIONS

1. **Background.** The Joint Chiefs of Staff approved new THREATCONs expanding the threat levels from three to four and recommending security measures for each threat level. Reference (c) implements the new Joint Chiefs of Staff directive in a Chief of Naval Operations (OPNAV) instruction. Paragraph 0212 of reference (c) provides the recommended security measures to be taken for a corresponding THREATCON.

2. **Policy.** Security measures recommended for each THREATCON will be implemented, if possible, by all Naval Reserve commands upon receipt of a THREATCON warning for their installation or area.

3. **Responsibilities**
   
   a. Commanding officers may raise or lower the THREATCON for their commands based on locally evaluated threats. Commands will notify COMNAVRESFOR, via the chain of command, of any change in THREATCONs. Commanding officers will not lower THREATCONs set by higher authority.

   b. COMNAVRESFOR may raise or lower THREATCONs of subordinate activities based on analyzed threats.
CHAPTER IX

INFORMATION AND PERSONNEL SECURITY

1. **Background.** The increasing number of espionage cases dictate that commands ensure policies and procedures for protection of classified information and material are understood and practiced effectively.

2. **Policy.** Commands will ensure that the requirements of reference (b) are met and that there is strong command support for information and personnel security program.

3. **Responsibilities**

   a. COMNAVRESFOR (Code 01A2) is responsible for the COMNAVRESFOR Information and Personnel Security program and will:

      (1) provide policy, direction, and guidance to field activities on implementation of the information and personnel security program,

      (2) ensure through oversight inspections that field activities are conducting their information and personnel security program per the requirements of reference (b),

      (3) with COMNAVRESFOR (Code 003), review cases of possible compromise and ensure preliminary inquiries and/or Judge Advocate General investigations are conducted as required, and

      (4) provide technical expertise to field activities on matters relating to the information and personnel security program.

   b. Commanders/commanding officers of Echelon III, IV, and V commands will:

      (1) provide command support for an effective information and personnel security program,

      (2) appoint a Security Manager, in writing, to coordinate and manage the command’s personnel and information security program,

      (3) ensure the individual designated as the security manager has completed the required training and is knowledgeable of their responsibilities.

      (4) designate a Top Secret Control Officer, in writing, if the command handles Top Secret information, and

      (5) designate an Automated Information Systems Security Officer, in writing, if the command is involved in processing data in an automated system.
COMNAVRESFORINST 5500.3A

5 FEB 1993

c. Command security managers shall:

(1) serve as the commanding officer’s advisor and direct representative in matters pertaining to information and personnel security,

(2) prepare written command procedures for the handling, safeguarding, accountability, and destruction of classified materials. An Emergency plan must be included as part of the procedures/plan. COMNAVRESFOR (Code 01A2) will provide a generic information/personnel security plan with emergency procedures annex upon request.

(3) formulate and coordinate the information security education program for the command,

(4) ensure compliance with classified material accounting and control requirements, including receipt, distribution, inventory, reproduction, and disposition,

(5) formulate and coordinate physical security measures for protection of classified material,

(6) ensure personnel security investigations are initiated and tracked to completion; clearances and access are recorded and limited to personnel with a need-to-know,

(7) ensure continuous evaluation of the trustworthiness, loyalty, reliability, and judgment of personnel who hold security clearances,

(8) collect data related to personal foreign travel as per reference (b). Ensure personnel are advised of the requirement to report personal foreign travel during orientation briefings and annual refresher briefings. When travel patterns or failure to report such travel indicates the need for investigation, refer the matter to the nearest Naval Criminal Investigative Service-office for action and to COMNAVRESFOR (Code 01A2) for information,

(9) ensure technical surveillance countermeasures sweeps are requested when required by reference (q),

(10) conduct oversight inspections of subordinate activities to ensure compliance with reference (b) and this instruction, and,

(11) initiate preliminary inquiries into possible compromise situations and process as necessary via the chain of command per reference (b). COMNAVRESFOR (Code 01A2) will be provided a copy of all preliminary inquiries.

4. Security Manager Decimation

a. Personnel designated as the Security Manager will have completed, prior to appointment, one of the following courses of instruction:
(1) NAVEDTRA correspondence course 13080 (Security Manager).

(2) Naval Criminal Investigative Service Command’s Mobile Training Team Course S-3C-001 (Security Manager’s Course).

(3) Section 3.6 of the Reserve Center Commanding Officer’s Course (R-07A-0010) beginning with the January 1993 session.

(4) COMNAVRESFOR Information/Personnel Security seminar beginning with the first seminar in 1993.

b. COMNAVRESFOR (Code 01A2) will entertain requests for waivers for the above requirements, for up to six months, based on substantiating documentation as to why one of the courses could not be completed prior to appointment. This requirement is effective six months from the date of this instruction.

c. Individuals will be appointed as security manager using the format of Exhibit IXA. The commander, commanding officer, or officer-in-charge will ensure the designated security manager signs and returns a certification of completion of a required course of instruction, and provides an acknowledgment of their responsibilities and duties, as well as certification that a complete inventory and turn over (with any discrepancies noted) has been completed. Exhibit IXB provides a sample format to be used for this certification.

5. Control of classified material will be accomplished per the procedures established in Appendix D. Existing systems may continue to be used until 1 July 1993 to ensure accuracy and accountability of documents received during that period.

6. OPNAV Form 5510/413 (Personnel Security Action Request) shall be submitted to the Department of the Navy Central Adjudication Facility for revalidation of a security clearance whenever an individual transfers from the activity holding his/her service record, and exercising administrative jurisdiction, to another activity. Within the Naval Reserve, such transfer is considered to have occurred when the individual transfers from one Reserve activity (Reserve center/facility, inshore undersea warfare unit, cargo handling battalion, mobile construction battalion, shore intermediate maintenance activity, squadron, air Reserve center, air Reserve activity) to another activity. Transfer within such activities does not require the revalidation of the security clearance.
EXHIBIT IXA
LETTER OF DESIGNATION

From: Commanding Officer
To: (Name, Rate/Rank/Grade, SSN)

Subj: DESIGNATION AS COMMAND SECURITY MANAGER

Ref: (a) OPNAVINST 5510.1H
     (b) COMNAVRESFORINST 5500.3A

1. You are hereby designated the command Security Manager and will familiarize yourself with the requirements of references (a) and (b). You will ensure that the duties and responsibilities, as outlined in Chapter II, paragraphs 2 through 8 of reference (a), are carried out to the best of your ability. You will assess the status of the program and provide a written report detailing any deficiencies. You will ensure all aspects of the program are coordinated with the appropriate individuals and that all command personnel are kept abreast of changes in policies and procedures and provided assistance in solving security related problems.

2. You are to assure all applicable OPNAV 5510 Notices are held by the command and are maintained until incorporation into reference (a).

(SIGNATURE)

IX-A-1
EXHIBIT IXB
CERTIFICATION OF TRAINING AND
ACKNOWLEDGEMENT OF RESPONSIBILITIES

From: (Name, Rate/Rank/Grade, SSN)
To: Commanding Officer

Subj: CERTIFICATION OF TRAINING AND ACKNOWLEDGEMENT OF RESPONSIBILITIES

Ref: (a) COMNAVRESFORINST 5500.3A
     (b) OPNAVINST 5510.1H

1. I have completed the (specify the course of instruction) as required by reference (a). I am fully aware of the duties and responsibilities of the position as outlined in Chapter II, paragraphs 2 through 8 of reference (b). A complete inventory of the command’s classified holdings has been accomplished and (specify if all material has been accounted for and if any discrepancies exist in the program).

2. I have assumed responsibilities for all classified materials and will ensure accurate and complete accountability of all classified materials held by the command.

(SIGNATURE)
CHAPTER X

LOSS PREVENTION

1. **Background.** The Navy has long recognized the importance of a vigorous loss prevention program and the need of loss trend analysis to determine where, when, and how property-losses occur. Such losses cost the Navy millions of dollars annually and at times prevent the timely accomplishment of our mission. Losses must be minimized by the application of a comprehensive loss prevention program.

2. **Policy.** Commands shall establish a comprehensive loss prevention program per the requirements of reference (c), and ensure all government owned property which is Missing, Lost, Stolen or Recovered (MLSR) is reported per the requirements of reference (p).

3. **Responsibilities**
   
   a. COMNAVRESFOR (Code 01A2) shall review and analyze MLSR government property reports submitted per reference (p) and develop an annual trend analysis on these losses, as well as provide recommendations for reducing or eliminating losses.

   b. Commanding officers shall develop and maintain an effective and comprehensive loss prevention program to protect command assets from theft and pilferage. These shall include the following elements.

      (1) **Loss analysis** - A review and analysis of all losses experienced by the command to help identify trends and patterns. Losses which do not require a MLSR report or Report of Survey under the MLSR program shall be included in the review process.

      (2) **Investigative and police resources** - Command investigative personnel shall be used to investigate incidents of loss or theft of government property and to assist in loss prevention efforts. Areas where highly valued, pilferable or sensitive property is stored should be patrolled frequently by security force personnel to discourage theft and assist in apprehending any perpetrators.

      (3) **Loss prevention equipment** - Commensurate with the value and sensitivity of the structure’s contents, appropriate doors, hardware, locks, and security devices shall be provided to prevent theft and/or pilferage.

      (4) **Employee education** - The command’s security education program shall include indoctrination in local procedures for preventing property losses, as well as employee’s responsibilities for care and protection of government property under their control/custody.
(5) Disciplinary and financial responsibility - Ensure proper disciplinary and/or pecuniary actions are taken when a loss of government property is due to negligence or disregard of established procedures, instructions, or statutes.

(6) Loss reporting - MLSR government property reports will be submitted promptly as required by reference (p). The command security officer shall be the focal point for tracking such reports. COMNAVRESFOR (Code 01A2) will be included as an addressee on all MLSR reports. Reports shall be submitted in the approved format and contain the information outlined in reference (p).

(7) Key and lock control - Commands shall establish a strict key and lock control program managed and supervised by the activity security officer. The Navy Lock and Key Control Guide (Ashore), prepared by the Navy Civil Engineering Laboratory, shall be used in establishing and maintaining a key and lock control program.

(8) Intrusion detection systems - New intrusion detection systems (IDS) will comply with Chapter 8 of reference (c) or Chapter 7 of reference (n), as applicable. Prior to procurement and installation of IDS, the plans will be sent to COMNAVRESFOR (Code 01A2) for review and approval. The plans will include:

(a) a diagram of the installation showing protected areas,
(b) list of parts, type, model, and manufacturer,
(c) cost for entire system (purchase and installation),
(d) cost of monitoring and who will monitor,
(e) cost of maintenance contract, and
(f) name and address of supplier.

4. All equipment and suppliers must be approved by Underwriters Laboratory.

5. Existing IDS will be maintained in optimum condition. It is generally beneficial to have a service contract with a reputable firm for this purpose.
CHAPTER XI

LAW ENFORCEMENT/SECURITY OFFICE FORMS

1. **Background.** CNO directed a reorganization of law enforcement and physical security programs under one program manager. Standardization was recognized as the greatest need to enhance professionalism. The first area to be standardized was the forms used for reporting law enforcement incidents. Forms used in support of law enforcement activities, such as visitor’s passes, vehicle passes, vehicle registration forms, were not included in the standardization process. A review of such forms used by COMNAVRESFOR Security Department indicates that each activity has developed locally produced forms of this nature. This practice violates the concept of standardization and cost effectiveness, as well as Navy regulations on forms management.

2. **Policy.** All COMNAVRESFOR Security Departments will use the following forms in lieu of locally produced forms:

   a. OPNAV 5560/1 (Rev 7-78) Non-Government Vehicle Registration - to be used for recording the necessary information to issue vehicle identification stickers.

   b. CNET-GEN 5512/8 (Rev 3-77) Temporary Vehicle Pass - to be used for identification of vehicles being authorized temporary access to a Naval Reserve installation.

   c. CNET-GEN 5512/3 (Rev 3-77) Pass Application - to be used for recording the necessary information to issue permanent identification passes (OF-55) to non-military government and contract personnel.

   d. OPTIONAL FORM 55 (6-73) U.S. Government Identification - to be issued as the identification media for non-military government and contract personnel.

   e. NAVRES 5532/1 (5-84) Visitor and Vehicle Registration Log - to be used for registering the issuances of temporary vehicle and visitor’s passes.

   f. NAVRES 5580/1 (4-90) Deadly Force Certification - to be used as a record of acknowledgement by Navy Security Force personnel that they have read, understand, and will comply with U.S. Navy Regulations on the Use of Deadly Force.

3. **Responsibilities.** Command security officers shall ensure that the prescribed forms are used in security departments and that these forms are not reproduced locally except when it is deemed to be in the best interest of the Navy or the limitations of time makes it essential.
CHAPTER XII

BOMB THREATS

1. Background. Militant groups, anarchists, criminal elements, and scores of others have manufactured and used explosives and incendiary devices in their rebellion against “the establishment.” Bombing and threats of bombing have created a need to properly plan for such threats and incidents.

2. Policy. All COMNAVRESFOR activities will establish procedures for handling bomb threats and for prohibiting the introduction of explosive devices into or around areas occupied by such activities. Command physical security plans shall include an annex on bomb threats which incorporates the provisions of Appendix B to this instruction.

3. Responsibilities

   a. Commanding officers will designate an individual as a “Bomb Scene Officer” who will be delegated full authority to handle all decisions relating to the bomb threat. This person could be the Command Duty Officer or Officer of the Day.

   b. Commands will organize a bomb search team to ensure the orderly and complete search of all areas if a bomb threat is received.
CHAPTER XIII

FLIGHTLINE PHYSICAL SECURITY

1. **Background.** This chapter isolates relative physical security requirements, and identifies individual and organizational security responsibilities to ensure an acceptable flightline security posture aboard all COMNAVRESFOR stations/facilities. References (c) through (n) support this chapter and issue specific security standards for aviation assets and shall be used for specific station/facility security issues.

2. **Policy.** Naval Air Stations and Naval Air Facilities under the cognizance of COMNAVRESFOR shall ensure security measures outlined in this chapter and in references (c) and (d) are enforced and jurisdictional control is exercised in such a manner to ensure maximum effective security within the following constraints:
   
   a. Available forces and resources.
   
   b. Variations in the threat or degree of threat in different geographical areas and operations.
   
   c. Specific activity/tenant unique real estate controls and jurisdictional issues and operational requirements.
   
   d. Federal, state, and local governmental agency rules and regulations that are individual station/facility peculiar issues.

3. **Responsibilities**
   
   a. COMNAVRESFOR (Code 01A2) is responsible for:
      
      (1) Providing guidance, planning and management expertise to all levels of command relative to aviation assets security.
      
      (2) Monitoring compliance with the physical security/law enforcement requirements of this instruction and references (c) through (g).
      
      (3) Submitting Program Objective Memoranda issues in support of the Aviation Asset Security Upgrade Program and ensure the support of COMNAVRESFOR for these issues.

   b. Commanding officers will ensure the establishment of an Aviation Asset Security Program (AASP) per Appendix C and references (c) and (d) to include:
      
      (1) An AASP plan which addresses viable flightline security procedures and which details accurate and realistic standards,
(2) security forces which are properly trained in aviation asset crisis action procedures and are exercised and drilled, and

(3) other related physical security procedures and programs which are supportive of flightline security.
CRIME PREVENTION

1. **Background.** The Navy has long felt the impact of crime on its military and civilian personnel and communities in which they live. Crime not only hurts the victim, it also adversely impacts the command to which the individual is attached. Work quality and productivity are diminished, victims suffer fear and anxiety and lose days from work. With their proven effectiveness in reducing crime and losses, crime prevention programs are capturing increasing Navy interest. This attention may be explained in part by the fact that crime prevention programs, in many cases, not only reduce crime, but also act as stepping stones to a more productive workplace and a healthier community.

2. **Policy.** Crime prevention is a command responsibility. A successful program requires continuing command emphasis and involvement. Commanding officers can reduce crime rates at their activities and reduce corresponding distractions from command readiness. Commands will develop and implement crime prevention programs which inform and protect potential victims and warn would-be offenders.

3. **Responsibilities**

   a. COMNAVRESFOR (Code 01A2) will ensure activities are provided up-to-date information and crime prevention training material upon request. A crime prevention pamphlet will be developed and disseminated to Reserve activities.

   b. Commanding officers will establish crime prevention programs within their commands which inform and protect potential victims and warn would-be offenders. A successful crime prevention program should include:

      (1) Realistic quantitative objectives. Establish objectives which are challenging but obtainable. Involve all levels of command and staff in the development of objectives.

      (2) Establishment of clear strategies including education, deterrence, and enforcement.

      (3) Active liaison with Naval Criminal Investigative Service, local law enforcement agencies, and other appropriate agencies for exchange of crime prevention related information.

      (4) Participation in crime prevention campaigns to highlight specific crime problems.
c. Commanding officers must continually evaluate crime trends and develop appropriate strategies based on their analysis. This ongoing analysis should aid commanding officers in tailoring crime prevention programs to deal with recurring current criminal activity. Commanding officers should use their analysis to identify high risk targets and initiate proactive measures to prevent crime.

d. A Crime Prevention Council will be established at Naval Air Stations/Naval Air Facilities and the Naval Support Activity, New Orleans, Louisiana. The Crime Prevention Council should assist commanding officers in establishing objectives and strategies to reduce crime affecting their installation.

e. Crime Prevention Councils should use the expertise of the Navy security department or local law enforcement agencies to assist in analyzing crime data, identifying major problem areas, and developing possible countermeasures.

f. Crime Prevention Councils should consider recommendations of the Navy security department during development of objectives and strategies. A positive, fully coordinated, and command supported crime prevention program should reduce the incidence of crime in Naval communities.
CHAPTER XV

SAFEGUARDING NORTH ATLANTIC TREATY ORGANIZATION
(NATO) CLASSIFIED MATERIAL

1. Background. The security requirements established by reference (b) normally provide sufficient safeguards to protect classified information from unauthorized disclosure. However, certain programs require additional protection and special handling procedures because of the sensitivity of material involved. Such additional measures are required for the protection of NATO classified material per reference (r).

2. Policy. Each Naval Reserve command that receives, holds, and/or distributes NATO classified material must adhere to the requirements of references (b) and (r), as well as this instruction.

3. Responsibilities. COMNAVRESFOR (Code 01A2) is the NATO subregistry for all Naval Reserve activities and is responsible for management and coordination of the program to safeguard NATO classified material assigned.

   a. COMNAVRESFOR (Code 01A2) is assigned administrative and oversight responsibility. This includes:

      (1) Establishing NATO Control Points (NCP) per reference (r). Only commands required to hold NATO secret material will be designated. These will be decided on a case-by-case basis.

      (2) Establish NATO User Offices where activities do not have a requirement for receipt, dispatch or retention of NATO classified material over a long period of time.

      (3) Conducting inspections of echelon III and IV commands to ensure adequate guidance, assistance, and oversight to subordinate activities.

      (4) Providing guidance as necessary.

   b. Echelon III and IV commands are responsible for the operation of this program at their own command and at subordinate commands. They are responsible for:

      (1) Conducting and documenting inspections of NCP on an annual basis per reference (r). In the interest of limiting expense and promoting efficiency, these inspections may be done by someone colocated at the command, or from a nearby command. Inspectors must be active duty commissioned officers, enlisted personnel E7 through E9, or a civilian employee GS9 or above. A final United States secret clearance is required.

XV-1
(2) Inspecting other commands that hold NATO classified material per the normal three year inspection cycle. Inspection guides will reflect procedures used to inspect NATO classified materials at subordinate activities.

(3) Ensuring compliance with accounting and control requirements for NATO material to include receipt, distribution, inventory, reproduction, and disposition.

4. Action

a. All commands that hold NATO classified material will:

(1) Ensure personnel authorized access to NATO material have been granted a final United States clearance. Interim clearances may not be used as a basis for access to NATO classified material.

(2) Provide personnel requiring access to NATO classified material an indoctrination brief (Appendix E, Part 1 provides a sample brief). This includes inspectors of NCP.

(3) Ensure combinations to security containers used to store NATO material are changed semiannually; when subjected to compromise; or when an individual holding the combination no longer requires access, or transfers from the organization.

(4) Maintain NATO material separately from other documents/material except Naval Warfare Publications which are allowed to be intermingled.

(5) Maintain an up-to-date roster of individuals authorized access to NATO material.

(6) Develop a written emergency destruction and/or evacuation plan that includes the following specific instructions:

(a) Who authorizes evacuation or destruction,

(b) What form of transportation will be used and who will provide for movement of the documents,

(c) Where will the documents be moved to and/or destroyed, and

(d) How accountability records (i.e., registers, inventories) should be secured.

(e) Ensure incidents which lead to the possibility of compromise or actual compromise of NATO classified material are reported through the chain of command to COMNAVRESFOR (Code 01A2) within 72 hours of occurrence.
Provide servicing communication centers a list of individuals with NATO access who are authorized to receive NATO classified messages.

Ensure NATO electrical messages are receipted for and controlled in the same manner as other NATO documents.

Ensure debriefs are given to personnel with NATO access upon reassignment or whenever there remains no-requirements for continued NATO access.

b. Commands designated NCP:

1. Designate, in writing, an NCP Officer and alternate(s). These appointments shall be restricted to active duty, full time support personnel.

2. Complete the Subregistry/Control Point Signature List (DWG Form 29) signed in black ink only. A new DAAG Form 29 must be prepared anytime there is a change of NCP officers or alternates. Submit the original form to COMNAVRESFOR (Code 01A2).

3. Inventory NATO secret documents annually and upon relief of the NCP officer or alternate.

5. Inspection/Inventory. The annual inspection/inventory of an NCP will be accomplished by 31 December and documented in detail. A copy of the inspection/inventory will be sent to COMNAVRESFOR (Code 01A2) by 15 January. Part 2 of Appendix E will be used as a guide to conduct and document the inspection. The inventory will list NATO secret documents by title/subject.
CHAPTER XVI
REPORTING REQUIREMENTS FOR SUPPORT TO CIVILIAN LAW ENFORCEMENT OFFICIALS

1. **Background.** It is the Department of the Navy’s policy to cooperate with civilian law enforcement officials to the maximum extent practicable, consistent with the needs of national security and military preparedness, the historic tradition of limiting direct military involvement in civilian activities, and the requirement of applicable law.

2. **Policy.** Upon request, Naval Reserve commands may provide support to civilian law enforcement efforts that are clearly within the purview of reference (a). Any law enforcement assistance that is not covered by reference (a), or requires a significant expenditure of government funds on a non-reimbursable basis, must receive approval by the next senior in the chain of command.

3. **Action.** Commands providing support to civilian law enforcement officials will submit quarterly reports detailing the support provided and the cost associated with such support. The reports will be submitted in the format prescribed by enclosure (1) to reference (a). Reports must be submitted by the fifth day of the month following the end of each quarter. Negative reports are not required.

   a. COMNAVRESFOR (Code 01A2) will be responsible for the collection and correlation of information from throughout the Naval Reserve and the submission of a quarterly report to the Chief of Naval Operations (N-515).

   b. Commander, Naval Air Reserve Force (Code 519) will provide information on aviation resources used in support to civilian law enforcement officials. This information shall be provided to the COMNAVRESFOR Security Office for inclusion in the quarterly report.
CHAPTER XVII

COMBATING TERRORISM

1. **Background.** Reference(s) establishes Department of the Navy (DoN) policy for the protection of DoN personnel, family members, resources, facilities, and equipment against terrorist acts and directs the elevation of awareness to the general terrorist threat by advising personnel, through an Anti-Terrorist Awareness Program, of terrorist threats in their assigned areas. Reference(s) also requires personnel ordered to a designated high-physical threat or potential physical threat country, for temporary duty, receive terrorist threat awareness and travel security briefings prior to departure. Units deploying to designated countries must also receive briefings.

2. **Policy.** Naval Reserve commands will establish a combating terrorism program tailored to the local mission, conditions, and terrorist threat.

3. **Responsibilities.** Commanding officers will initiate action to inform, train, educate, and protect military and civilian personnel and resources from terrorist acts to include:
   
   a. Providing a terrorist threat awareness, personal protection, and pre-departure travel security briefing prior to the commencement of travel outside the continental United States (except Alaska and Hawaii). Personnel traveling to or through a DoD-designated high-physical threat or potential physical threat country will also receive the above briefings prior to commencement of travel. The Pre-Departure Education Lesson Topic Guide (Appendix F), with the video tapes “Hard Target” and “Self Protection Measures Against Terrorist” shall be used in the development and conduct of the required briefings.
   
   b. Providing annual security briefings to personnel who frequently travel overseas.
   
   c. Incorporating anti-terrorism protection measures and contingency plans in the installation/activity physical security plan.

4. COMNAVRESFOR (Code 01A2) will provide, upon request, up-to-date information on DoD-designated high-physical threat or potential physical threat countries as well as information on the DoN Anti-terrorist Alert Center’s Terrorist Threat Levels. This information may be obtained telephonically by contacting the COMNAVRESFOR Security Office at DSN 363-1951/52 or commercial (504) 948-1951/52.
APPENDIX A

COURSE OF INSTRUCTION
AUXILIARY SECURITY FORCE (ASF)

1. The purpose of this course of instruction is to train designated naval personnel in the basic physical security knowledge and skills required to perform security sentry duties and defend against terrorist activity as members of an ASF. The course is designed to provide the ASF member with an acceptable level of knowledge and skills required of an armed sentry capable of using deadly force.

2. ASF qualification training will be conducted in two phases, Phase I will consist of 40 hours of academic subjects and practical exercises; Phase II is 40 hours of weapons training. Phase I and II will be conducted consecutively thereby making the initial training program 80 hours in length. Phase I and II instruction will be presented by qualified Marine Corps Security Force Cadre personnel assisted by local command instructors, or a Mobil Training Team provided by the Marine Corps. Methods of instruction will include lectures, demonstrations and practical exercises to enhance member’s understanding of instructional subjects and reinforce learned physical skills. On conclusion of Phase I training, the member will be required to successfully pass a written and practical examination to demonstrate the member’s mastery of physical security knowledge/skills presented during Phase I. ASF members who fail to successfully complete Phase I requirements will be excluded from further ASF training and replacement from the parent command is required. At the conclusion of Phase II training, the ASF member will be required to successfully complete a written examination and practical weapons qualification course to demonstrate mastery of weapons knowledge and skills presented during Phase II. Results of written/practical examinations and weapons qualifications will be recorded in the member’s training record and be made available on request.

3. The installation’s ASF will be organized along lines that will promote unit integrity and support the installation’s security mission. The organization may be developed to permit unit type deployment for riot/civil disturbance mission. Organization planning must also consider the requirement to conduct a continuous revolving ASF training program to train members as they are assigned.

4. Phase I and II training will be conducted in a consecutive two week period. ASF members will be required to stand duty a minimum of eight hours per month, preferably two four hour shifts, to maintain proficiency.

5. Each ASF member will have a training record. At a minimum, the record will document subjects or courses of instruction, instructor’s name, dates of completion, hours of instruction, examination results, weapons scores, expiration dates of pertinent certifications, licenses and permits. Individual training records will be forwarded with the individual upon transfer.

A-1
(reverse blank)
The training syllabus for ASF training Phases I and II are as follows:

**PHASE I (Physical Security)**

<table>
<thead>
<tr>
<th>SUBJECT</th>
<th>HOURS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duties/function of the Security Department</td>
<td>.50</td>
</tr>
<tr>
<td>Legal jurisdiction and authority</td>
<td>.50</td>
</tr>
<tr>
<td>Interior guard duties and orders</td>
<td>1.00</td>
</tr>
<tr>
<td>Search techniques</td>
<td></td>
</tr>
<tr>
<td>- personnel</td>
<td>1.00</td>
</tr>
<tr>
<td>- vehicles</td>
<td>1.00</td>
</tr>
<tr>
<td>- buildings</td>
<td>1.00</td>
</tr>
<tr>
<td>- areas</td>
<td>1.00</td>
</tr>
<tr>
<td>Use of force</td>
<td></td>
</tr>
<tr>
<td>- DON policy</td>
<td>1.00</td>
</tr>
<tr>
<td>- rules of engagement</td>
<td>1.00</td>
</tr>
<tr>
<td>Unarmed self defense</td>
<td>4.00</td>
</tr>
<tr>
<td>Activity security department communications</td>
<td>1.00</td>
</tr>
<tr>
<td>Individual tactics</td>
<td></td>
</tr>
<tr>
<td>- cover</td>
<td>.75</td>
</tr>
<tr>
<td>- concealment</td>
<td>.75</td>
</tr>
<tr>
<td>- movement</td>
<td>.50</td>
</tr>
<tr>
<td>Search and seizure</td>
<td>1.00</td>
</tr>
<tr>
<td>Uniform Code of Military Justice</td>
<td>1.00</td>
</tr>
<tr>
<td>Apprehension and restraint</td>
<td>1.00</td>
</tr>
<tr>
<td>Crowd control</td>
<td>1.00</td>
</tr>
<tr>
<td>Anti-terrorism awareness</td>
<td></td>
</tr>
<tr>
<td>- personal protection</td>
<td>1.00</td>
</tr>
<tr>
<td>- surveillance protection</td>
<td>1.00</td>
</tr>
<tr>
<td>- threat type</td>
<td>1.00</td>
</tr>
<tr>
<td>Basic first aid</td>
<td>2.00</td>
</tr>
<tr>
<td>Community relations</td>
<td>1.00</td>
</tr>
<tr>
<td>Protection of crime scene</td>
<td>1.00</td>
</tr>
<tr>
<td>Disaster and emergency plans</td>
<td>3.00</td>
</tr>
<tr>
<td>Review and examination</td>
<td>2.00</td>
</tr>
<tr>
<td>Physical training (one hour daily)</td>
<td>5.00</td>
</tr>
<tr>
<td>Special subjects unique to the installation</td>
<td>4.00</td>
</tr>
</tbody>
</table>

**TOTAL** 40.00
### PHASE II (Combat Marksmanship Skills)

<table>
<thead>
<tr>
<th>SUBJECT (Pistol)</th>
<th>HOURS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pistol course introduction</td>
<td>.50</td>
</tr>
<tr>
<td>Pistol nomenclature and function</td>
<td>1.00</td>
</tr>
<tr>
<td>Pistol safety and handling</td>
<td>1.00</td>
</tr>
<tr>
<td>Weaver stance and grip</td>
<td>1.00</td>
</tr>
<tr>
<td>Pistol principles of target engagement</td>
<td>.50</td>
</tr>
<tr>
<td>Combat marksmanship principles</td>
<td>.50</td>
</tr>
<tr>
<td>Pistol reloading</td>
<td>1.00</td>
</tr>
<tr>
<td>Pistol condition 3 presentation</td>
<td>1.00</td>
</tr>
<tr>
<td>Pistol immediate action</td>
<td>1.00</td>
</tr>
<tr>
<td>Pistol live firing drills (daylight)</td>
<td>15.00</td>
</tr>
<tr>
<td>(qualification - 2.00 hours)</td>
<td></td>
</tr>
<tr>
<td>Pistol night firing techniques</td>
<td>1.00</td>
</tr>
<tr>
<td>Pistol live firing drills (night time)</td>
<td>2.00</td>
</tr>
<tr>
<td>(qualification - 1.00 hours)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SUBJECT (Shotgun)</th>
<th>HOURS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shotgun course introduction</td>
<td>.50</td>
</tr>
<tr>
<td>Shotgun nomenclature and function</td>
<td>1.00</td>
</tr>
<tr>
<td>Shotgun safety and handling</td>
<td>1.00</td>
</tr>
<tr>
<td>Ammunition, patterning and aiming</td>
<td>1.50</td>
</tr>
<tr>
<td>Shotgun reloading</td>
<td>1.00</td>
</tr>
<tr>
<td>Carrying/shooting</td>
<td>1.50</td>
</tr>
<tr>
<td>Shotgun immediate action</td>
<td>1.00</td>
</tr>
<tr>
<td>Shotgun live firing drills</td>
<td>7.00</td>
</tr>
</tbody>
</table>

**TOTAL** 40.00
1. **Prevention.** Tightened security and controlled entry cannot be over-emphasized when dealing with potential bomb threat situations. Package control measures should be initiated. Locate and eliminate likely hiding places. Buildings should be inspected on a regular basis to reduce the possibility of a bomb being placed and also to minimize the time required for the search after a threat has been received.

2. **Planning and Preparation.** Only with a properly organized plan will those affected by a bomb threat know how, when and in what order to proceed. A list should be prepared of individuals and commands that must be notified and of emergency services that should be called to the scene. A bomb search team should be organized and trained to ensure the most thorough and expeditious search of all areas. Commanding officers will designate one officer as a “Bomb Scene Officer,” having authority for all decisions relating to bomb threats. Decisions as to credibility of the bomb threat, whether to evacuate and whether to re-enter the threatened area should be made by the bomb scene officer. Effective means of communication must be established in advance to ensure the most expeditious and orderly flow of information between the various elements involved. A minimum number of individuals should relay information on the progress of bomb searches, evacuation, and handling of suspect articles. Radio transmitters must be avoided as they could detonate an explosive. Careful planning will ensure rapid and effective communications between the bomb scene officer, search teams, and security and emergency team personnel. Bomb threat plans should address, at a minimum, the following factors:

   a. Control of the operation.
   b. Evacuation of all spaces.
   c. Search.
   d. Finding the bomb or suspected bomb.
   e. Disposal - Explosive Ordnance Detachment (EOD).
   f. Detonation and damage control.
   g. Control of publicity.
   h. Erection of barriers.
   i. Disconnection of utilities.
   j. Removal of flammable substances/explosives.
3. **Receiving a Threat**

In preparation for the eventuality of a telephone bomb threat, all personnel who handle incoming calls should be supplied with OPNAV 5527/8 (Telephone Threat Complaint). Personnel should be directed to remain calm and concentrate on the exact wording of the message, any background noises, any jargon or slang used by the caller, and any other details that may help establish who the caller may be. Personnel should attempt to obtain from caller the location of the bomb, when the bomb is to detonate, what the bomb looks like, and any other information that may assist in the bomb search. Personnel should play on the sympathy of the caller by voicing concern for injury or death the bomb could cause if detonated.

b. Personnel who handle mail should be briefed on the characteristics of letter and postal bombs and procedures established for handling any suspect items. Extreme caution must be emphasized in handling suspect packages and letters. Periodic re-briefs should be conducted to ensure personnel are aware of threats that exist and procedures to be used.

4. **Reporting a Bomb Threat.** Every bomb threat will be reported by the receiving command to COMNAVRESFOR and other commands as appropriate using the OPREP-3 Navy Blue reporting procedures. The nearest Naval Investigative Service element will be immediately notified to facilitate counter-intelligence and investigative assistance.

5. **Control of Operation.** The bomb scene officer should be given complete authority and responsibility for all matters relating to the bomb threat. A command post or control center should be established and at a minimum it should be manned by the following personnel:

a. The bomb scene officer.


c. Facilities Engineer or Public Works Officer.

d. Public Affairs Officer.

6. **Threat Evaluation.** When evaluating a bomb threat, the bomb scene officer should consider the following factors:

a. The content and specificity of the threat.

b. The degree of security and accessibility maintained by the activity.

c. Whether immediate evacuation will expose activity personnel to greater danger.
d. The number of personnel who must be evacuated.

e. Whether the caller is merely attempting to disrupt normal work routine or is genuinely aware of a bomb and is attempting to warn the activity in order to minimize potential injuries.

7. Courses of Action. Once the credibility of the bomb threat has been determined, four possible courses of action are open to the bomb scene officer:

a. do nothing,

b. search without evacuating (overt and covert),

c. partial evacuation and search, and

d. total evacuation and search.

8. Evacuation. Once the bomb scene officer has decided that the bomb threat is of a serious nature, proper authorities and fire and medical personnel have been contacted and it has been determined that at least a partial evacuation is necessary, the following steps should be followed:

An initial brief search must be made of established evacuation routes (usually fire evacuation routes) to prevent taking activity personnel through potential bomb location areas.

b. An evacuation signal should be sounded.

c. Prearranged evacuation routes should be followed. Alternate routes should be used to move personnel away from any area the caller has noted as a bomb location.

d. Certain members of the activity should be designated as members of the evacuation team. These individuals should guide activity members to the proper exit routes. They must maintain control to avoid panic and possible injury. Some evacuation team members should control access to the bomb area once it has been cleared.

9. Search Procedures. The following factors must be considered when conducting the search.

a. If a search is made without evacuating activity members, each area should have a member of the search team assigned to direct the search and maintain communications with the command post.

b. Search team members should be familiar with their areas and must be reminded that they are searchers and not bomb experts.
c. The search should proceed from outside to inside, bottom floor to top floor, more public areas to least public areas, and from floor to ceiling, unless specific information is received as to the location of the bomb.

d. The search teams should keep the command post informed as to the status of their search.

10. **Action Required if a Suspected Bomb is Found.** Should a suspicious object be found, the command post should be notified immediately and the Explosive Ordnance Disposal (EOD) dispatched to the area. Search team members should never attempt to do anything with a suspected bomb. The EOD has the responsibility to deactivate and remove the bomb. Should an explosion occur, no attempt to tamper with the debris should be made except to remove injured personnel. Evacuate remaining personnel and secure the area until EOD and security officials can take control. Ensure that a Naval Criminal Investigative Service representative is notified in all cases in which a bomb is found or detonated.

11. **Re-entry After an Evacuation.** If the building or area has been evacuated, re-entry must not be permitted until the entire area has been searched and no devices were found or the EOD has removed any devices found. The decision to re-enter should be made by the bomb scene officer.

12. **After Action Report.** A report and an evaluation of the incident should be made by the bomb scene officer for use in reviewing the local activity’s bomb threat plan.
APPENDIX C

PART 1

FLIGHTLINE PHYSICAL SECURITY

1. The air station/facility commanding officer is designated the single coordinating authority for the AASP. As such, the commanding officer is responsible for:

   a. Establishment and maintenance of security procedures which provide for protection of aviation assets. Such procedures shall include, but are not limited to, designation of Flightline/Support Facilities (F/SF) (e.g., aircraft, control towers, hangars, ramps, and communications equipment), restricted areas, station/facility perimeter security, pedestrian and vehicle control, internal roving patrols, administrative inspections, integrated communications, and back-up security force capability.

   b. Development, maintenance, and operational control of a personnel and vehicle F/SF identification and access control system.

   c. Establishment and maintenance of a single coordinated F/SF security force program including:

      (1) Navy Security Forces (NSF).

      (2) Auxiliary Security Forces (ASF).

      (3) NSF/ASF training (i.e., weapons qualifications, rules of engagement, deadly force requirements, and records keeping).

      (4) Periodic exercises to evaluate effectiveness.

   d. Establishment and maintenance of a station/facility-wide security education program (references (c) and (b) refer) which will ensure the awareness and involvement of all station personnel, host and tenant, in the AASP.

   e. Development and maintenance of facility host-tenant, Inter-Service Support agreements relative to specific F/SF security responsibilities and/or procedures.

2. The station/facility security officer is the commanding officer’s direct representative, responsible for managing and directing the overall F/SF security program.

3. All department/division directors are responsible for providing, as required, applicable fair share support services, facilities, equipment, and personnel to properly accomplish F/SF security requirements.
MINIMUM FLIGHTLINE PHYSICAL SECURITY STANDARDS

1. The following flightline physical security standards and requirements are established to ensure uniform minimum levels of security for COMNAVRESFOR mission critical aviation assets and F/SF. Station/facility commanding officers shall ensure that these standards are established and maintained. During increased terrorist threat conditions, air shows, and periods of civil unrest, these standards shall be upgraded to meet existing local conditions and resource availability.

2. The minimum physical security standards and policies are:

   a. All F/SF activities shall be designated and posted as Level TWO restricted areas within the applicable portions of reference (c). Major tenant activities shall be responsible for properly designating and posting their respective areas. Navy signs, as specified in Chapter 3 of reference (c), will be used to designate restricted areas by all activities, host and tenant.

   b. Points of F/SF ingress/egress shall be kept to the minimum required for safe and effective airfield operations and:

      (1) All gates shall be locked when not in use.

      (2) Infrequently used gates shall be fixed with car ball seals per reference (c).

      (3) Remote controlled Motorized Vehicular Gates and pedestrian turnstiles may be used for F/SF ingress/egress.

      (4) Locks, seals, and remote control devices shall be strictly controlled and monitored by the facility security officer. Inventories of these items shall be accomplished at least semiannually.

   c. An F/SF personnel access control system shall be established per Part 4 of this Appendix.

   d. An F/SF vehicle access control procedure shall be established per Part 6 of this Appendix.

   e. Specific station/facility directives concerning control of photography shall be developed. In general, camera equipment will not be allowed within F/SF areas unless specifically authorized; however, photographs are allowed during air shows/open house events.
3. The following minimum personnel requirements will be adhered to:

   a. A minimum of one supervisor (E5 or above, rated Master at Arms or Navy Enlisted Classification (NEC) code 9545 qualified, or Department of Defense civilian GS-083/085) who is weapon qualified, will be on watch at all times.

   b. A minimum of two armed, mobile personnel are on watch within the flightline or can respond within three to five minutes to F/SF security situations. One individual will be armed with a shotgun.

   c. A minimum of a five-person security force element, each armed and with proper communications, shall be available to respond to emergency F/SF situations within 15 minutes.

4. The following minimum personnel training requirements will be met:

   a. All personnel not normally assigned to NSF or ASF security duties shall receive and successfully complete, at a minimum, the training required for ASF members.

   b. F/SF crisis action drills shall be developed and conducted semiannually, with one of these drills being a night exercise. Corrective action on lessons learned shall be documented and maintained for three years. These drills may stand alone or be held with other station security department drills.

5. Aviation assets security upgrades, as described in Appendix IX, Part 1 of reference (c), will be implemented at the earliest possible date. Projects for these upgrades will be developed per the Security Upgrade Plans provided by the CNO (N-09N). Special projects and military construction, Naval Reserve projects shall be submitted per chapter II of this instruction and reference (h).
TENANT ACTIVITY SUPPORT RESPONSIBILITIES

1. As outlined in reference (c), the host station/facility commanding officer has overall physical security coordinating responsibilities within the confines of the installation, including F/SF. In support of this responsibility, tenant activities (squadrons, communications-services, supply activities, U.S. Customs offices, U.S. Coast Guard facilities, and U.S. Army activities) shall ensure compliance with this instruction and accomplish/provide the following:

   a. Per references (c) and (b), designate a security officer in writing who will be the single point of contact to develop an activity physical security plan and ensure the plan is integrated into the host installation Physical Security Plan.

   b. Establish and maintain a strict key and lock program for the internal protection of spaces and equipment.

   c. Provide the host activity with a list of personnel/vehicles requiring badges/passes for F/SF access per Parts 4 and 6 of this Appendix.

   d. Where required (local host determination) establish and maintain a visitors log of personnel authorized F/SF access.

   e. Ensure personnel receive periodic host security awareness training and that all tenant personnel are knowledgeable of and comply with host activity F/SF security procedures.

   f. Review and update ISSAs as required.

   g. When requested by the host activity, ensure F/SF personnel access badges are produced, distributed, and accounted for.

2. Tenant activities are responsible for the internal security of their spaces. Tenant activity sponsored security watches shall be coordinated with the host activity.
FLIGHTLINE PERSONNEL CONTROL PROCEDURES

1. Personnel access to F/SF areas will be strictly controlled per this instruction and reference (c). Commanding officers of air stations/facilities are responsible for overall F/SF personnel control procedures and shall ensure compliance with the following standards and requirements:

   a. Personnel requiring daily job related F/SF access shall be allowed entry to F/SF areas upon presentation of a valid F/SF badge.

   b. Access to F/SF areas will not be authorized on the basis of rank, uniform markings, or military identification card (DD2N or DD2N(Res)), including other corresponding military or civilian dependent identification cards or documents.

   c. Host activity commanding officers will allow visiting/transiting aircrews and personnel, with valid home station badges, access to local common use (parking ramps, air operations, and weather/aerology) flightline spaces. Host commanding officers may require a badge exchange system for other restricted access areas such as intelligence spaces and operational control centers.

   d. Host activity commanding officers shall develop local procedures for authorizing other visiting/transiting military/civilian government aircrews and/or personnel F/SF access. The intent of these policies shall be to ensure compliance with the provisions of this instruction and provide for close and compatible working relationships with U.S. Air Force, U.S. Marine Corps, U.S. Army, U.S. Coast Guard, U.S. Customs, and Drug Enforcement Agency personnel and mission requirements.

   e. Host activity commanding officers shall determine local station/facility policies concerning responsibility for badge preparation, distribution, and accountability. Stations may direct the security department to prepare, distribute, and control all F/SF badges or may elect to have tenant commands prepare and distribute badges used by their personnel, with the host security department responsible for all F/SF badge accountability, confiscation, and turn-in actions.

   f. Tenant activities shall comply with the provisions of this instruction, and provide the host with appropriate support to implement F/SF personnel control procedures as outlined in respective ISSA and host F/SF security implementing directives.

2. All F/SF personnel ingress/egress points will be marked with distinctive signs indicating that all hand carried parcels and vehicles are subject to search at anytime within the F/SF area. Host activities shall ensure that random administrative inspections are conducted at least weekly per reference (c). Administrative inspections will be increased, as determined by the host activity, upon designation of THREATCON Alpha or above.
1. All COMNAVRESFOR F/SF access identification badges shall conform to the following characteristics:

   a. The basic badge shall be:

      (1) White in color with black printing.

      (2) The same size as the standard U.S. military identification card before laminating (2-1/8" X 3-1/4" (57mm x 82mm)). Locally printed blanks shall be compatible with existing photographic equipment.

      (3) The photograph shall be a color, head and shoulders on a cream color background, minimum size 1" x 1-1/4" (25mm x 30mm).

      (4) A clear space at the top of the badge/pouch will be provided to place a hole for an attachment device.

   b. The front of each badge will have:

      (1) A separate serial number (individual station/facility determination).

      (2) Blocks numbered 1 through 7 will be printed to the left, and blocks 8 through 14 will be printed to right (facing badge) of the photograph (see sample on page C-9).

      (3) Space for the name of the holder, which must be typewritten.

      (4) The holder shall sign his/her name over the name block.

      (5) Space for the holder’s activity/command.

      (6) Space for the holder’s rank, rate, or grade.

      (7) Space for a badge expiration date.

      (8) Space for the name of the station/facility issuing the badge.

      (9) Space for the name, title, and signature of the issuing officer.

   c. The back of each badge will have:

      (1) Space for the issuing activity logo, if desired.
(2) Space for the date of badge issue.

(3) Space for a notice - "Warning: For Official Use of the holder identified thereon. Use or possession by any other person is unlawful and will make the offender liable to penalty under 18 U.S.C. 49, 506, and 701."

(4) Space for statement “If found return to the nearest U.S. Armed Forces installation or drop in nearest U.S. Mail Box.”

(5) Space for statement “Postmaster: Postage Guaranteed: Return to Commanding Officer (address of issuing activity).”

(6) Space for activity’s form number

d. Block numbers indicated in paragraph 1b(2) above will be standardized for the following F/SF areas:

(1) Left Side

(a) Block 1, air operations

(b) Block 2, weather/aerology

(C) Block 3, supply

(d) Block 4, AIMD (includes avionics)

(e) Block 5, fuel

(f) Block 6, weapons

(g) Block 7, communications/antennas

(2) Blocks (8) through (14) on the right side, will be used by the host activity to identify tenant commands i.e., Intelligence, U.S. Customs, U.S. Coast Guard, Marine Air Groups, Wings, and Squadrons) requiring access to F/SF areas.

Unused and unauthorized access block numbers will be blackened out (black ink over number block within lines).

f. Badge lamination will be a heat seal type that would disfigure the face of the badge and picture upon attempted separation.

g. Two types of visitor badges are authorized and will be configured from serialized badges described above. All visitor badges will be marked with a red “V” over the picture area.

(1) Unescorted (locally approved) visitor’s badges will be marked with a green “U” annotated on the lower right of the badge face.
(2) Escort required (locally determined – except where noted in this instruction) visitor’s badges will be marked with a red “E” annotated in the lower right of the badge face.

2. Station/facility commanding officers shall determine local procedures and responsibilities relative to the production, distribution, accountability, and safeguarding of F/SF access badges. Such procedures shall ensure a log is maintained indicating badge serial number, holder’s name, date issued, area(s) authorized access, date returned, and holder’s signature.

3. F/SF access badges will be issued to:

   a. United States military personnel (all services, active duty, and Reserve) for the period of duty the service member requires F/SF access and/or is expected to remain at the host activity, but no longer than six years from date of issue,

   b. United States government employees for the period the employee requires F/SF access at the host activity, but no longer than six years from date of issue.

   c. Contractors, vendors, and equipment service representatives requiring:

      (1) At a minimum, weekly (once a week) F/SF access, may be issued F/SF badges. In these cases, the word contractor and the company name must be typed in the station logo area on the back of the badge. Contractor badges may be issued for the duration of the contract, and/or service requirement, but in no case longer than two years from date of issue.

      (2) Infrequent contractor F/SF access requirements (less than weekly) will be processed as either unescorted or escorted visitors.

   d. Dependents will be issued escorted visitor badges and will be escorted by the sponsoring activity.

4. Badges will be worn on the outer garment, upper torso, with photograph facing forward while in the F/SF area (badges need not be worn while working on aircraft if foreign object damage conditions exist).

5. F/SF badges will not be displayed when outside the F/SF area.

6. The host activity will establish accounting procedures for lost badges. When six percent of F/SF badges are lost or unaccounted for, badges will be reissued. In any case, F/SF badges will be reissued every six years from initiation of the host activity F/SF badge program.

7. The host activity will conduct an F/SF badge inventory by serial number of in stock and issued badges at least every 12 months.
1. Responsibility for control of vehicle access in the F/SF area rests with the installation commanding officer. In this capacity the commanding officer shall:

   a. Establish a viable F/SF security program that provides for the detection, delay, and/or denial of unauthorized vehicles (and persons) to aviation resources. This program shall be designed to ensure that all F/SF personnel become and remain knowledgeable of their individual and unit security responsibilities.

   b. Establish, maintain, and man all F/SF vehicle ingress/egress control points. Ingress/egress points will be kept to the absolute minimum in consonance with aircraft operations and safety requirements.

   c. Establish F/SF vehicle access, control, pass, and parking procedures.

   d. Properly post and maintain F/SF vehicle ingress/egress points and parking areas per reference (c).

   e. Ensure F/SF vehicle access, control, pass, and parking procedures are identified in the station/facility security plan and meet the provisions of reference (c).

   f. Provide for and maintain a vehicle identification and pass system.

   g. Enforce F/SF vehicle rules, regulations, and restrictions.

   h. Establish and maintain random F/SF vehicle administrative inspection procedures per reference (c).

2. F/SF tenant activities shall:

   a. Ensure compliance with the host station/facility vehicle control program.

   b. Incorporate host station/facility vehicle control procedures into the tenant activity security plan.

   c. Provide, as required by the host, information deemed appropriate to allow for F/SF vehicle access on a tenant unique base (i.e., specific equipment repair, change of command, and single source vendor visit).
d. Provide escorts for vehicles requiring F/SF access when requested by the host activity.

3. Host activity F/SF vehicle control procedures shall as a minimum:

   a. Require that all vehicles be positively identified prior to accessing F/SF spaces.

   NOTE: Standard government (federal, state, and county) vehicle markings are adequate for F/SF access during non-THREATCON status. More restrictive procedures may be established by the host activity. Unmarked government rented/leased vehicles shall be identified by a clearly visible (from outside the vehicle) placard (no less than 5" x 10") placed on the dash or sun visor. The host activity shall determine strict enforceable procedures for issuance, accountability, and disposition of these type passes. Host or supporting activity emergency vehicles (fire, crash/rescue, police, and medical) shall be allowed immediate access to the F/SF emergency scene unless more restrictive measures are established by the host activity.

   b. Require all vehicle occupants be positively identified prior to accessing F/SF spaces. Procedures outlined in Part 4 of this appendix shall be used as basic personnel identification/control procedures. More restrictive measures may be established by the host activity.

   c. Require that a log-in/log-out system be established using NAVRES 5532/1 forms and the forms be maintained for two years.

   d. Ensure F/SF vehicle placards/passes are distinctly different size, color, and markings from regular station/facility visitor vehicle access passes.

   e. Require visiting vehicle escort system at THREATCON Charlie, unless more restrictive procedures are established by the host.

   f. Require, where applicable, procedures for the issue, use, and control of motorized vehicular gates.

   g. Require procedures for the establishment of routine, random administrative inspections in an F/SF area as part of the host activity counter-intelligence, anti-terrorism and loss prevention program.

   h. Prohibit privately owned vehicles from entering or parking within F/SF or along barriers or clear zones. This requirement may be waived during special events (i.e., air shows, scout jamboree, and changes of command).

   i. Establish procedures for the identification and control of commercial contractor vehicles relating to F/SF access.
APPENDIX D

ACCOUNTABILITY AND CONTROL OF CLASSIFIED MATERIAL

1. Basic Concept. To provide information with a level of accounting and control required by its assigned security classification. This is accomplished by:
   a. limiting dissemination of material,
   b. preventing unnecessary duplication of material, and
   c. identifying the person or office directly responsible for security of the material.

2. Accounting and Control
   a. By definition, certain distinctions exist between the three levels of classification (Top Secret, Secret, Confidential) therefore, so does the degree of accounting and control required. Classified materials will be accounted for and controlled as follows:
      (1) Top Secret. Any command holding Top Secret material must:
         (a) Designate, in writing, a Top Secret Control Officer (TSCO). The TSCO is responsible for receiving, maintaining accountability, distribution, and destruction of Top Secret material.
         (b) Ensure that the quantity of Top Secret material is kept to a minimum.
         (c) Provide “cradle-to-grave” accountability. A hand-to-hand continuous chain of receipt is required, even within the command.
         (d) Ensure there is a record of individuals who have had access to Top Secret material - e.g., an OPNAV Form 5511/13 (Record of Disclosure) is maintained for each Top Secret document to identify every individual who has seen or handled the document, including administrative and clerical staff.
         (e) Prohibit the reproduction of Top Secret material without the consent of the originator or higher authority.
         (f) Ensure all records pertaining to the accounting and control of Top Secret material are retained a minimum of five years after the document is destroyed, transferred, or downgraded.

   (2) Secret. Accountability and control of Secret material will include all materials originated and received by the command and will be controlled using the automated database tracking system that has been
developed by COMNAVRESFOR. This system is based on a DBase III+ format database file, and is designed to be as simple and user-friendly as possible. The operator can select from several functions available at the main menu. These functions include adding new records, editing existing records, marking a record to show destruction, and printing reports. Upon entering receipt of new material into the program, the next consecutive control number will automatically be assigned, and the operator will enter appropriate information into designated fields. When finished entering all new materials, operator will have the option of viewing new records for accuracy and printing a listing of only the new materials entered. The system then automatically updates the active database, and a material control card is automatically printed. The Classified Material Control Form (NAVRES 5511/5) will be printed on #110 stock blank tractor-feed 8 1/2" x 5 1/2" cards. Two cards will be printed for each control number (an original and a routing copy). Upon destruction, the operator will be able to enter destruction for an individual control number, and the system will automatically remove that control number from the active database and insert it into a history database. Printed report options will include a full listing of active control numbers, a listing of control numbers by office codes, and a history of destroyed materials (full listings or by year). Control numbers will be attached to the actual material by means of a formatted, self-adhesive label. The target date for distribution of the program is set for 31 March 1993, mandatory use will be required by 01 July 1993 (unless modified by COMNAVRESFOR (Code 01A2)).

(3) Confidential. While the requirements for Confidential material are less stringent, procedures must be followed to protect it from unauthorized disclosure by access control as well as compliance with marking, storage, transmission, and destruction requirements.

b. Top Secret, Secret, and Confidential are the only classification categories. Although some materials require specific administrative procedures (e.g. Naval Warfare Publication Library, NATO, Safeguarding the Single Integrated Operational Plan-Extremely Sensitive Information), those procedures do not replace requirements for proper protection under reference (b). For example, a Secret Naval Warfare Publication (NWP), is a Secret document first, and an NWP second.

c. Material originated within the command, working papers or notes must be afforded the basic level of protection required for its classification level, including but not limited to being dated when created, marking on each page reflecting the highest level of classification assigned, protected per its classification, and destruction by authorized means when no longer required. Working papers must be protected by all accounting, control, and marking requirements if they: contain Top Secret material; are held onboard more than 90 days; are to be filed permanently; or are released outside the command.

d. All Top Secret and Secret material transferred out of the command must be logged, and shall include as a minimum, the serial number, date, addressee, and date receipt returned.
3. Transmission of Classified Material

a. Top Secret material may not be transmitted through the mail. Chapter 15 of reference (b) provides specific guidance for transmission of Top Secret material.

b. Secret material may be mailed by United States Registered Mail within and between the United States and its territories and through Army, Navy, or Air Force Postal Service facilities provided the material remains under United States control (i.e., it does not pass through a foreign postal system, any foreign inspection, or via foreign airlines).

c. Confidential material may be mailed by United States First Class mail between DoD activities anywhere in the United States and its Territories. Whenever First Class mail is used to transmit Confidential material, the outer envelope must be marked with the words "Postmaster: Do Not Forward, Return to Sender" and "FIRST CLASS" (or "PRIORITY MAIL" if the package weighs over 12 ounces). United States Registered Mail is required for NATO Confidential and any Confidential mailed to and from Army Post Office or Fleet Post Office addresses outside the United States and its territories. Mailing the material to DoD contractors or non-DoD agencies of the Executive Branch requires the use of United States Certified Mail.

d. Classified material must be addressed only to an official government activity or DoD contractor, NOT to an individual. When it is appropriate to direct material to the attention of an individual or code, this should be indicated on an attention line on the inner envelope only. Consult the Standard Navy Distribution List for appropriate addresses.

e. Classified material will be enclosed in two opaque, sealed envelopes or similar wrappings, which are carefully sealed with brown paper sealing tape to minimize the possibility of access without leaving evidence of tampering. Transparent tape, electrical tape, and masking tape are not considered sufficient protection as they are easily removed and do not retain the impression of a postal stamp.

f. Material will be folded or packed so the text will not be in contact with the inner envelope or container.

g. Inner envelope: will show the address of the receiving activity, highest classification of the material enclosed, and any other markings or special instructions (such as "Restricted Data"). Return receipt for Secret material will be attached to the inner envelope.

h. Outer envelope: will contain the full Standard Navy Distribution List address of the receiving activity and return address of the sending activity. It will not contain any markings, listing of the contents divulging classified information, or any other unusual data or marks which might invite special attention to the fact that contents are classified.
NATO CLASSIFIED MATERIAL BRIEFING GUIDE

1. General
   
a. The information in this guide is based on NATO Security Policy and Procedures and is for the purpose of briefing all personnel who will have access to NATO documents classified SECRET and below.

   b. Such personnel must first be cleared for access to the same level of United States classified information and must be aware of their responsibility and to the consequences of negligence (see Appendix F of reference (b)). There is no such thing as a ‘NATO’ clearance.

2. Security Grading. The word ‘NATO’ is a marking which, when applied to a document, signifies that the document is the property of the International Pact Organization and, if bearing a security grading, must not be passed outside of the organization and is subject to security protection issued, per reference (r).

3. Application of NATO Markings
   
a. The marking ‘NATO’ will be applied to all copies of documents prepared for circulation within the International Pact Organization. Under no circumstances should it be applied to United States documents within United States agencies.

   b. Where approved channels are used for interchange of NATO information between the United States and NATO agencies, only the last United States agency having custody of the information is authorized to apply the appropriate marking.

   c. The security classification, together with the NATO marking, should appear on the top and bottom of each page of a document and each page should be numbered.

   d. NATO documents must be typed, translated, and reproduced only by those persons who have been granted access to NATO classified information.

4. Access on a Need-to-know Basis. Access to NATO classified information must be confined to those whose duties make such access essential. No person is entitled solely by virtue of rank or appointment to have access to NATO classified information. In each and every case the need-to-know must be established, and will be determined by the individual having possession, knowledge, or command control of the information involved, and not by the prospective recipient.
5. **Security in Buildings**

   a. Access to all offices in which there are NATO documents must be controlled by:

   (1) A pass or personnel recognition system, including arrangements for receiving visitors.

   (2) Making the office secure from unauthorized entry.

   b. Visitors must not be left unattended in individual offices or other designated areas containing NATO material.

   c. Places in which there are NATO documents must be inspected at the end of normal working hours to ensure that safes, cabinets, and spaces are locked; and documents\classified waste are securely housed.

6. **Extracts and Reproduction**

   a. Extracts of NATO documents may be included, if necessary, in United States papers requiring action by persons who have not been authorized to have access to NATO information. Such extracts will not be marked with the pact marking. To ensure that the extracts are properly protected, such papers must be given an appropriate United States security classification and must be distributed only on a need-to-know basis.

   b. Reproduction of NATO documents is authorized provided all security precautions prescribed for the original documents are observed with respect to the reproduction.

7. **Packaging**

   a. When NATO documents are to be transmitted from one agency to another or one command to another, the double wrapped system will be used. A receipt, if required, will be enclosed.

   b. The receipt, OPNAV Form 5511/10 (Record of Receipt), which requires no security grading, should quote only reference number of document and not the title.

   c. The inner cover will be sealed and enclosed in a sealed outer cover. Under no circumstances will the security grading appear on the outer cover. A diplomatic pouch may be considered as the outer cover.

   d. When NATO documents are carried by hand between offices within the same building, they must be covered in such a way as to prevent observation of their contents.
8. **International Transmission.** NATO documents may be conveyed by diplomatic pouch, military courier service, registered United States military postal system or through the Canadian military postal system, or other military postal systems as approved by NATO.

9. **National Transmission**
   
   a. Transmission of NATO documents between points within the United States jurisdiction may be sent by United States registered mail.

   b. Whenever a messenger service is used for NATO documents to be carried outside the confines of a building, packaging must meet the provisions in subparagraphs 7a, b, and c above.

10. **Security of Courier Personnel.** All couriers and messengers employed to carry NATO documents must be security cleared by the employing agency.

11. **Electronic Transmission**
   
   a. NATO messages will be given protection at least equivalent to that of other documents with the same classification.

   b. Telephones may not be used for the discussion of classified information.

12. **Safe Custody of NATO Documents**
   
   a. Documents, when not in use, will be safeguarded per the provisions of reference (b), for United States documents of commensurate classification. Security measures per paragraph 5 above, will be taken.

   b. Whenever an office is left unattended during normal working hours, NATO documents must be returned to storage.

   c. Do not combine NATO material with other classified material in file cabinets.

13. **Maintenance of Clearance List.** An up-to-date list of individuals having authorization for access to NATO documents will be maintained by the office responsible for dissemination of classified material. All such personnel will certify in writing that they fully understand security regulations pertaining to the handling of NATO documents.
APPENDIX E
PART 2

NATO INSPECTION CHECKLIST

1. ORGANIZATION AND LOCATION:
2. DATE OF INSPECTION:
3. CONTROL POINT PERSONNEL CONTACTED:
4. TOTAL NUMBER OF DOCUMENTS:
   NATO SECRET:
5. POSSIBLE COMPROMISE/BREACH OF SECURITY:
   a. Number Reported:
   b. Number handled locally:
6. NAME, RANK/RATE/GRADE OF INSPECTOR:
7. REMARKS:

Referenced paragraphs are from OPNAVINST C5510.101D (USSAN 1-69 of 21 Apr 82).
******ADMINISTRATION******

1. Is a copy of last years inspection report on file?

2. Has corrective action been accomplished?

3. Is USSAN Instruction 1-69 or applicable publication containing the provisions of the USSAN Instruction on file with activity?

4. Are the control officer and alternate(s) designated in writing? (Paragraph 116, Attachment 1; Paragraph 27, Attachment 2).

5. Is there a written emergency evacuation and/or destruction plan? (Paragraph 114-115, Attachment 1).

6. Is the Specimen Signature List (DAAG Form 29) current? (Paragraph 127, Attachment 1; Paragraph 27, Attachment 2).

7. Are control personnel aware of their reporting responsibilities in the event of an actual or possible compromise? (Paragraph 147-161, Attachment 1; Paragraph 4-16, Annex v, Attachment 2).

8. Upon change of Control Officer, is there a 100 percent joint inventory of NATO secret documents conducted (Paragraph 100, Attachment 1; Paragraph 31c, 33c, Attachment 2).

9. Has coordination been made with the supporting communications center for handling of all NATO messages (Name of supporting communications center).

* * * * * * PHYSICAL SECURITY * * * * * *

1. Are security areas and containers inspected at the end of each workday? (Paragraph 52, Attachment 1).
2. Are storage facilities the same as prescribed for storage of United States material of the same classification? (Paragraph 56, Attachment 1).

3. Are keys and combinations to security containers afforded commensurate protection with the level of material safeguarded? (Paragraph 59, Attachment 1).

4. Are combinations to security containers changed when appropriate? (Paragraph 60, Attachment 1).

5. Installation Security (Check appropriate item)
   a. Guarded _____ (By Whom) _____ Open _____
   b. Perimeter _____ Wall _____ None _____

6. Control Point Building Security (Check appropriate item)
   a. Construction: Masonry_____ Metal _____ Wood _____
   b. Floors: Single _____ Multiple_____
   c. Entry: Escort_____ Pass _____ Unrestricted_____ 
   d. Windows: Alarmed _____ Barred _____ None _____
   e. Guards: Internal _____ External _____ None _____
       Duty Hours _____ Mil _____ Civ _____
       If patrol, how often_________
   f. Perimeter: Fence _____ Wall _____ Other (explain)

7. Control Point Spaces (Check appropriate item)
   a. Door: Metal _____ Wood _____ With Locks (Comb _____
       Key _____ Padlock _____)
   b. Windows: None _____ Protected _____ Unprotected _____
   c. Access: Controlled _____ Uncontrolled _____
   d. Alarm System: Contact _____ Motion _____ None _____
   e. Document Storage: Vault _____ Security container _____

***** PERSONNEL SECURITY *****

1. Are individuals granted access to NATO classified material based on their equivalent United States clearance? (Paragraph 30, Attachment 1).
2. Are individuals briefed prior to being granted access to any level of NATO classified information (Paragraph 33, Attachment 1; Paragraph 53, Attachment 2).

3. Are current lists of individuals authorized access to NATO classified information maintained at each office where such information is stored and in the office authorizing access (Paragraph 39, Attachment 1; Paragraph 31, Attachment 2).

4. Are debriefing certificates retained for a period of one year (minimum) following termination of duties requiring access? (Paragraph 44, Attachment 1; Paragraph 53, Attachment 2).

5. Are debriefings conducted on all individuals ceasing to be employed in duties requiring access? (Paragraph 44, Attachment 1; Paragraph 53, Attachment 2).

****** DOCUMENT CONTROL ******

1. Are all NATO documents and messages filed/stored separately from non-NATO material? (Paragraph 56, Attachment 1).

2. Are requests and/or reports of reproduction, micro-filming, or translation of NATO secret documents forwarded to the CUSR? (Paragraph 89, Attachment 1; Paragraph 43, Attachment 2).

3. If documents are reproduced, are proper procedures followed in the control of all drafts, copies, and waste, and in the reproduction facilities? (Paragraph 89, Attachment 1; Paragraph 43-45, Attachment 2).

4. Are exercise documents and messages handled properly? (Paragraph 100 and 109a and b, Attachment 1; Paragraph 50-52, Attachment 2).
5. Have internal administrative procedures been established to record the internal movement of NATO SECRET material? (Paragraph 100, Attachment 1).

6. Are there procedures established for the personal carriage of NATO material? (Paragraph 108, Attachment 1).

7. Have procedures been established to identify material for destruction which is no longer required? (Paragraph 112-113, Attachment 1).

8. Are NATO SECRET certificates of destruction being maintained for two years after being executed by two properly briefed officials? (Paragraph 113, Attachment 1).
COURSE TITLE: Navy Combating Terrorism Program
Pre-Departure Education

CLASSIFICATION: Unclassified

LESSON TOPIC NUMBER: 1.1

LESSON TOPIC: Pre-Departure Education

ALLOTTED LESSON TIME: 1.0 Period

INSTRUCTIONAL REFERENCES:
1. SECNAVINST 3300.2
2. OPNAVINST 3300.53

INSTRUCTIONAL VIDEOS:
1. Hard Target (Pin No. 803445DN)
2. Self Protective Measures Against Terrorists, Part 1 (Pin No. 804720DN)

TERMINAL OBJECTIVE:
(Supported in part by this lesson topic)

1.0 To provide guidance and information for the protection of Navy military and civilian personnel and family members worldwide against terrorist acts.

ENABLING OBJECTIVES:
(Completely supported by this lesson topic)

1. Select statements that identify tactics commonly used by terrorist groups.

2. Select statements that identify measures that will enhance personal security during travel.
I. INTRODUCTION

A. Lesson Objective

1. Select statement that identify tactics commonly used by terrorist groups.

2. Select statement that identify measures that will enhance personal security during travel.

B. Lesson Orientation

1. Importance of lesson content to student
   a. A very real threat exists for U.S. Navy facilities and personnel.
   
   b. Domestic and international terrorists have become very skillful in use of ruses and disguises that make it easier for them to observe, evaluate, and gain access to their targets.
   
   c. This lesson will present some of the strategies for protection of personnel with added caution that alertness, coupled with common sense and personal initiative, are the best deterrence to terrorist attacks against individuals.

2. Lesson Process
   a. Lecture
   b. Video

II. Presentation

A. Terms and Definitions

1. Terrorism - The calculated use of violence or threat of violence to create fear; intended to coerce or to intimidate government or societies in the pursuit of goals that are generally political, religious, or ideological.

2. Combating Terrorism - Actions, including anti-terrorism, taken to oppose terrorism throughout the entire threat spectrum.

3. Anti-terrorism - Defensive measures used to reduce vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

4. Counter-terrorism - Offensive measures taken to prevent, deter, and respond to terrorism.
5. DoD-Designated High Physical Threat Countries - Geographic areas determined to be of significant terrorist threat to DoD travelers as designated by the Assistant Secretary of Defense (Special Operations/Low Intensity Conflict) in coordination with the Assistant Secretary of Defense (International Security Policy) and the Deputy Undersecretary of Defense (Strategy and Resources). DoD-designated high-physical threat countries are listed in the Navy Anti-terrorist Alert Center (NAVATAC) Sunday Summaries.

B. Terrorist Profile

1. It is not accurate to say that there is a “typical” terrorist, but some of the characteristics that appear in many terrorists are:

   a. They are well trained in tactics and use of weapons
   b. They may be idealistic in their motivations
   c. They may be mentally unstable
   d. They have criminal motivations, without ideological political or religious aims
   e. They are often very dedicated to the cause of their organization
   f. Most terrorists are not suicidal

C. Terrorist Operations

1. Terrorist operations are generally:

   a. Designed to make an impact
   b. Well planned and organized
   c. Over in 6 to 60 seconds
   d. Successful

2. Most operations are conducted within a tight schedule

3. The target is generally lightly defended or unprotected

4. Targets are observed for some time before the attack occurs

   a. An alert security force member who stops a suspicious person for questioning can divert a terrorist attack
b. If a terrorist group sees that a base is randomly checking cars that come through the gates, the group may choose another target

5. Operations are generally rehearsed several times and may be called off if the target person or installation does something unexpected

6. Terrorist groups have been known to use disguises and ruses to conduct surveillance or attacks. They have disguised themselves as:

   a. Postal workers
   b. Priests and nuns
   c. Police
   d. Military
   e. Telephone repairmen
   f. Joggers
   g. Airline personnel
   h. Food/supply delivery

7. Tactics

   a. Bombings - May use bombs of any degree of sophistication placed to destroy equipment, cause fires, and create casualties

      (1) This is the most common tactic, accounting for more than 50 percent of terrorist incidents over the last two decades

      (2) Bombs are inexpensive and easy to make

      (3) They are delivered in a variety of ways

         (a) Vehicle bombs, including suicide bombs, placed in parked cars and devices intended to kill the driver and passengers

         (b) Sent through the mail, or put into the target site

   b. Hijacking

      (1) Hijacked vehicles give the terrorist a legitimate means with which to approach, or gain entry to a military installation

      (2) Hijacked airlines or cruise ships guarantee media coverage
c. Hostage taking

(1) Terrorists may take a hostage to a location away from the scene of the kidnapping

(2) They may stay at the scene for a direct confrontation with authorities

D. Protective Measures

1. Proper personal security measures are devised to lower your visibility and increase your survivability while traveling abroad. These measures can be summed as follows:

a. Knowledge: Being aware of the threat situation in the area to or through which you are or will be traveling.

b. Anonymity: Methods employed to prevent easy identification as a representative of the United States.

c. Foresight: Being prepared, both personally and professionally, for the possibility of a highjacking or other terrorist incident.

2. The following videos will provide specific recommendations to assist military members, their families, and DoD civilian employees in making travel procedures as safe as possible.

a. Show videos:

(1) Hard Target

(2) Self Protection Measures Against Terrorists

Video tapes may be obtained from the activities below using the PIN numbers indicated in the INSTRUCTIONAL AIDS section

Naval Education and Training Support Center, Atlantic
Code N5
Bldg. W-313, Fleet Branch
Norfolk, VA 23511-6197
DSN: 564-4011/1468
Commercial: (804) 444-4011/1468
or
Naval Education and Training Support Center, Pacific
Code N52
San Diego, CA 92132-5105
DSN: 522-1342/3345
Commercial: (619) 532-1342/3345

F-5
(reverse blank)